

---

**From:** Justin Brookman <[REDACTED]>  
**Sent:** Sunday, November 20, 2022 7:39 PM  
**To:** Regulations  
**Subject:** CPPA Public Comment  
**Attachments:** CPPA regs comments (Nov 2022).pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Attached please find Consumer Reports's comment on the CPPA's Modified Draft Regulations.

\*\*\*

This e-mail message is intended only for the designated recipient(s) named above. The information contained in this e-mail and any attachments may be confidential or legally privileged. If you are not the intended recipient, you may not review, retain, copy, redistribute or use this e-mail or any attachment for any purpose, or disclose all or any part of its contents. If you have received this e-mail in error, please immediately notify the sender by reply e-mail and permanently delete this e-mail and any attachments from your computer system.

\*\*\*

Comments of Consumer Reports  
In Response to the  
California Privacy Protection Agency on the  
Modified Text of Proposed Rules under the California Privacy Rights Act of 2020

By

Justin Brookman, Director of Technology Policy

November 21, 2022



Consumer Reports<sup>1</sup> appreciates the opportunity to comment on the modified proposed rules (the Modified Draft Regulations) interpreting the California Privacy Rights Act (CPRA).<sup>2</sup> We thank the California Privacy Protection Agency (CPPA) for soliciting input to make the California Consumer Privacy Act (CCPA),<sup>3</sup> as amended by Proposition 24, work for consumers.

The Modified Draft Regulations appear to have been changed largely to accommodate businesses who criticized the scope and text of the original Draft Regulations. While the CPPA certainly should consider ease and cost of compliance in promulgating its regulations, the Modified Draft Regulations have swung too far in the wrong direction. By removing certain provisions proscribing anti-consumer practices, the CPPA is signaling that behaviors previously prohibited by those provisions are now legitimate. We urge the CPPA to either undo certain revisions or make further revisions to ensure that the CPRA effectively protects California consumers.

#### § 7004. Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent.

We strongly disagree with the new language contained in § 7004(c) replacing “regardless of user intent” with “A business’s intent in designing the interface is not determinative in whether the user interface is a dark pattern, but a factor to be considered.” Setting aside the practical difficulty in proving subjective intent, business intent is *never* relevant in assessing whether a particular design is deceptive or not. The effect of the pattern on the user is the only relevant consideration. For this reason, intent is typically not an element of consumer protection laws such as federal and state prohibitions on deceptive and unfair business practices. A company’s intent may be a consideration for a regulator in deciding whether to bring an action or in determining the appropriate penalty in a settlement. It is not, however, a relevant consideration in determining whether a legal violation has occurred. We urge the CPPA to revert to the previous language.

We also urge the CPPA to revert the last two examples removed from § 7004(a)(2) and the first example removed from § 7004(a)(4). All three are straightforward examples of

---

<sup>1</sup> Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers’ interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

<sup>2</sup> California Privacy Protection Agency, Notice of Proposed Rulemaking, (Jul. 8, 2022), [https://cppa.ca.gov/regulations/pdf/20220708\\_npr.pdf](https://cppa.ca.gov/regulations/pdf/20220708_npr.pdf).

<sup>3</sup> For purposes of this comment, we will refer to the current text of California’s privacy law — as amended by the CPRA — as the CPRA. References to the CCPA are references to the original CCPA before it was amended.

deceptive dark patterns; removing them signals to industry that these practices are now considered legal and allowable under the CPRA. The two examples in § 7004(a)(2) are clear violations of the principle of “symmetry of choice” — in both, the options to allow data collection are obviously more prominent and asymmetrical. In § 7004(a)(4), forcing a user to agree to the likely factually incorrect statement of “I don’t like to save money” in order to decline consent for data collection is clearly abusive and unjustifiable. We also reiterate our suggestion from our previous comments where we urged the CPPA to specify that more prominent choices that lead to additional data collection are prohibited, while privacy-preserving options are allowed to be more prominent.<sup>4</sup>

#### § 7012. Notice at Collection of Personal Information.

We recommend restatement of § 7012(e)(6)’s requirement that companies provide either notice of specific third parties with whom they share data or a description of the third parties’ business practices. The provision already offered companies flexibility in either identifying companies or at least describing their practices to consumers. The CPRA requires companies to disclose the “categories” of third parties with whom data is shared; a description of third parties’ business practices is needed in order to make those categories comprehensible.

#### § 7013. Notice of Right to Opt-Out of Sale/Sharing of and the “Do Not Sell or Share My Personal Information” Link.

We recommend reinstatement of the examples deleted from § 7013(e)(3). Both are uncontroversial examples of the principle stated in § 7013(e)(3) that “A business shall also provide the notice to opt-out of sale/sharing in the same manner in which it collects the personal information that it sells or shares.” Deleting these examples from the draft regulations will lead to the implication that connected devices and virtual reality systems *do not*, in fact, need to provide notice in the same manner in which they collect personal information.

#### § 7016. Notice of Financial Incentive.

While the Modified Draft Regulations do not make any significant changes to this section, we remain disappointed that it does not provide clear guidance to companies or consumers as to what practices might violate § 125(b)(4) of the CPRA’s provision that a “business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.” We reiterate our previous remarks that the CPPA should clarify that offers should be presumed to be illegitimate in concentrated markets or markets for essential services,

---

<sup>4</sup> Comments of Consumer Reports In Response to the California Privacy Protection Agency on the Text of Proposed Rules under the California Privacy Rights Act of 2020, (Aug. 23, 2022), at 9, <https://advocacy.consumerreports.org/wp-content/uploads/2022/08/CPRA-regs-comments-summer-2022-1.pdf>.

and that companies should be required to provide an accounting of the “good-faith estimate of the value of the consumer’s data” as required by the CPRA.<sup>5</sup>

§ 7025. Opt-Out Preference Signals.

§ 7026. Requests to Opt-Out of Sale/Sharing.

In general, we support the new language in § 7025 clarifying that companies who receive an opt-out preference signal in one context must apply that opt-out in other contexts where it recognizes the consumer, account, or device. The revisions to the examples in this section are also helpful in this regard.

We also restate our suggestion that the CPPA consider hosting a registry of legally binding OOPS signals; we note that the Colorado Privacy Act draft regulations published last month commit the Colorado Department of Law to hosting and maintaining a comparable registry.<sup>6</sup>

However, we disagree with the changes to § 7025(c)(6) and § 7026(g) making it only optional for companies to provide notice to consumers that their opt-out choices have been honored. Failure to understand whether opt-out selections were effective or not was a common complaint from consumers who participated in Consumer Report’s crowdsourced study on the efficacy of opt-out rights.<sup>7</sup> We remained concerned that due to either technical malfunctions or simple malfeasance, consumers’ invocation of opt-out rights may not be effective in practice; a standardized notice that an opt-out has been recognized would help put consumers’ minds at ease.

We are especially worried about companies using dodgy interfaces to purportedly obtain consent to disregard generally applicable opt-out preference signals. For this reason, even if the CPPA does not want to require *every* company to display opt-out state, the CPPA should require that companies that *disregard* a recognized OOPS control — either because the company believes it has re-opt-in consent or because it does not believe the signal conforms to the CPRA’s requirements for an OOPS — must provide prominent notice to consumers that the OOPS is not considered operative. This approach would incentivize companies to respect OOPS signals and disincentivize bad faith efforts to generate spurious consent.

\*\*\*\*\*

---

<sup>5</sup> *Id.* at 10.

<sup>6</sup> *Id.* at 5. *See also* Colorado Department of Law, Consumer Protection Section, Colorado Privacy Act Rules 4 CCR-904-3, [https://coag.gov/app/uploads/2022/10/CPA\\_Final-Draft-Rules-9.29.22.pdf](https://coag.gov/app/uploads/2022/10/CPA_Final-Draft-Rules-9.29.22.pdf).

<sup>7</sup> Maureen Mahoney, *California Consumer Privacy Act: Are Consumers’ Digital Rights Protected?*, Consumer Reports, (Oct. 1, 2020), [https://advocacy.consumerreports.org/wp-content/uploads/2021/05/CR\\_CCPA-Are-Consumers-Digital-Rights-Protected\\_092020\\_vf2.pdf](https://advocacy.consumerreports.org/wp-content/uploads/2021/05/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf2.pdf).

We thank the CPPA for its consideration of these points, and for its work to secure strong privacy protections for consumers. We are happy to answer any questions you may have, and to discuss these issues in more detail. Please contact Justin Brookman [REDACTED] for more information.

---

**From:** privacyprosh [REDACTED]  
**Sent:** Sunday, November 20, 2022 9:18 PM  
**To:** Regulations  
**Subject:** CPPA Public Comment  
**Attachments:** Public comment on CPRA modified proposed regulations11.20.22.docx

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

CPPA Public Comment attached. Thank you for your consideration.

Sent with [Proton Mail](#) secure email.

November 20, 2022  
California Privacy Protection Agency  
Attn: Brian Soublet  
Submitted via e-mail to [regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)  
**CCPA Public Comment**

We respond below to the California Privacy Protection Agency's ("CCPA" or "Agency") Notice of modifications made to proposed regulations implementing the Consumer Privacy Rights Act of 2020 ("CPRA") by submitting written comments on the proposed modifications, specifically to propose certain additional modifications to the revised text of Proposed Regulations ("**Regulations**"). As the authorized representatives of a multinational e-commerce and online advertising company with a mid-sized California operation, we appreciate the opportunity to submit relevant comments for the Agency's consideration on behalf of this interested party.

### **INTRODUCTION**

Our comments focus on provisions in the Regulations that warrant additional revision so that the final Regulations will meet the OAL's substantive review standards (Authority, Reference, Consistency, Clarity, Nonduplication, and Necessity (Cal. Gov. Code §11349-11349.6)), and satisfy the Agency's mandate to implement regulations that are necessary to effectuate the CPRA, clarify interpretation, are consistent with the provisions of the statute and other regulations, do not exceed the Agency's rulemaking authority, and are feasible for affected parties to implement in a timely and cost-effective manner in order to effectively protect California consumers' privacy rights. Our suggested revisions and redlines to the Regulations are set forth at the end of each Section.

### **A. PROPOSED REGULATIONS SECTION 7002: RESTRICTIONS ON THE COLLECTION AND USE OF PERSONAL INFORMATION**

#### **1. Summary of Comment**

The examples provided in §7002(b) of the draft Regulations require their underlying assumptions to be expressly stated in order not to be misleading. In addition, the second example in §7002(b)(2) is too narrowly drawn and should be revised.



## 2. Substantive Reasoning for Recommended Revisions

Although the examples provided in §7002(b) are designed to provide guidance on the interpretation of whether a business's use of collected information is "reasonably necessary and proportionate to achieve" a disclosed purpose, these examples are misleading without the inclusion of certain assumptions critical to their understanding, namely that the other uses they deem unreasonable were either not disclosed to the user or do not meet the requirements of §7002(c). Without the inclusion of these assumptions, the effect of the examples in §7002(b) is to improperly imply that the consumer's intent in interacting with or using a business's product or service is the only relevant factor in the formation of their reasonable expectations, regardless of its disclosed purposes of collection, and thereby mistakenly imply that "consent" is required for any other use, even if such additional use was properly disclosed and meets the requirements in §7002(c). It is not a practical business requirement that every application, regardless of its disclosed purposes of collection, be customizable to fit only those uses that a particular consumer wants to make of it or the parts of its disclosed functionality that a consumer chooses to employ. Therefore, §7002(b) should be edited to include the assumptions on which the conclusions of its examples in (b)(1) – (b)(5) are based.

Moreover, the first example given in §7002(b)(2) is too narrowly drawn ("For example, if a business's mobile communication application requests access to the consumer's contact list in order to call a specific individual, the consumer who is providing their contact list likely expects that the purpose of the business's use of that contact list will be to connect the consumer with the specific contact they selected." Draft regulations §7002(b)(2)). As written, its implication would be that, after a contact list was used to enable a call to a particular contact in connection with which the list was first collected, either (a) the business would no longer have justification to retain the contact list, meaning it would need to be collected again each time the user wished to place a call to a particular individual on that list, or (b) the business would need to obtain the user's consent to thereafter use the contact list to place a call to any other particular individual on the contact list. This is highly impractical and likely not aligned with the user's reasonable expectations regarding the use of its contact list, which would instead include using

it to enable a call to any particular contact on the list at that time and thereafter, not just the original call. Thus, the first example in §7002(b)(2) should be revised and broadened.

### **3. Recommended Revisions to Regulations Section 7002**

We recommend editing §7002(b) to include the assumptions on which the conclusions of its examples in (b)(1) – (b)(5) are based, for example:

“(b) The purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer(s) whose personal information is collected or processed. **Provided that the additional purposes or uses described in the examples below were not disclosed and do not meet the requirements of subsection (c),** ~~the~~ consumer’s reasonable expectations concerning the **disclosed** purpose for which their personal information will be collected or processed shall be based on the following:”

We also recommend broadening the language of the first example in §7002(b)(2), perhaps as such:

“For example, if a business’s mobile communication application requests access to the consumer’s contact list in order to call a specific individual, the consumer who is providing their contact list likely expects that the purpose of the business’s use of that contact list will be to connect the consumer with ~~the specific contact they selected~~ **a contact they select from the contact list at that time or thereafter.**”

## **B. PROPOSED REGULATIONS SECTION 7027: REQUESTS TO LIMIT USE AND DISCLOSURE OF SENSITIVE PERSONAL INFORMATION**

### **1. Summary of Comment**

In §7027, collecting or processing sensitive information with the purpose of inferring characteristics about a consumer should be included separately as a pre-requisite to offering the option to limit, rather than as one of a list of exceptions in subsection (m).

### **2. Substantive Reasoning for Recommended Revisions**

As set forth in §7027(a), consistent with the statutory provisions in §1798.121(d), “Sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to requests to limit.” As such, the inclusion of this pre-requisite condition as number (8) in §7027(m)’s list of exceptions to the request to limit confuses and minimizes its nature as a requirement that gates the consideration of whether any of the other 7 exceptions listed in subsection (m) applies. Moreover, the Agency’s statutory mandate in to adopt regulations to further the purposes of the title expressly requires, in

§1798.185(a)(19)(C)(iv), “Ensuring that the exemption in subdivision (d) of Section 1798.121 for sensitive personal information applies to information that is collected or processed incidentally, or without the purpose of inferring characteristics about a consumer . . . .” Thus, in order to properly effectuate this mandate and provide clarity, the useful example from §7027 (m)(8) should be moved up to follow the last sentence in §7027(a), this condition should be pointed out explicitly as a pre-requisite to the requirement of offering the option to limit in both §7027(b) and §7027(m), and §7027(m)(8) should be deleted.

### **3. Recommended Revisions to Regulations Section 7027**

We recommend that the useful example from §7027 (m)(8) should be moved up to follow the last sentence in §7027(a), the condition of processing sensitive information with the purpose of inferring characteristics about a consumer should be pointed out explicitly as a pre-requisite to the requirement of offering the option to limit in both §7027(b) and §7027(m), and §7027(m)(8) should be deleted, such as the following:

“(a) The unauthorized use or disclosure of sensitive personal information creates a heightened risk of harm for the consumer. The purpose of the request to limit is to give consumers meaningful control over how their sensitive personal information is collected, used, and disclosed. It gives the consumer the ability to limit the business’s use of sensitive personal information to that which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services, with some narrowly tailored exceptions, which are set forth in subsection (m). Sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to requests to limit. **For example, a business that includes a search box on their website by which consumers can search for articles related to their health condition may use the information provided by the consumer for the purpose of providing the search feature without inferring characteristics about the consumer.**

“(b) **Unless a business collects or processes sensitive personal information without the purpose of inferring characteristics about a consumer, A** a business that uses or discloses sensitive personal information for purposes other than those set forth in subsection (m) shall provide two or more designated methods for submitting requests to limit. A business shall consider the methods by which it interacts with consumers, the manner in which the business collects the sensitive personal information that it uses for purposes other than those set forth in subsection (m), available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to limit. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer. Illustrative examples follow. . . .”

“(m) The purposes identified in Civil Code section 1798.121, subdivision (a), for which a business may use or disclose sensitive personal information without being required to offer consumers a right to limit are as follows. A business that only uses or discloses sensitive personal information **without the purpose of inferring characteristics about a consumer or** for these purposes **below**, provided that the use or disclosure is reasonably necessary and proportionate for those purposes, is not required to post a Notice of Right to Limit or provide a method for submitting a request to limit.

...

~~(8) To collect or process sensitive personal information where such collection or processing is not for the purpose of inferring characteristics about a consumer. For example, a business that includes a search box on their website by which consumers can search for articles related to their health condition may use the information provided by the consumer for the purpose of providing the search feature without inferring characteristics about the consumer.~~

## **C. PROPOSED REGULATIONS SECTION 7301(B): INITIATING INVESTIGATIONS**

### **1. Summary of Comment**

Proposed regulation §7301(b) regarding the Agency’s discretion to consider “all facts it determines to be relevant” in deciding whether to initiate an investigation lacks clarity as to how and when businesses could provide the relevant facts or information for the Agency to consider in making its determination, so the regulations should specify a forum or process for businesses to submit this information.

### **2. Substantive Reasoning for Recommended Revisions**

The OAL’s standard of review provides that a regulation is “written or displayed so that the meaning of regulations will be easily understood by those persons directly affected by them.” Cal Gov. Code §11349(c).

Draft regulation §7301(b) gives the Agency the discretion to “consider all facts it determines to be relevant, including the amount of time between the effective date of the statutory or regulatory requirement(s) and the possible or alleged violation(s) of those requirements, and good faith efforts to comply with those requirements,” in its determination whether to pursue investigations of possible or alleged violations of the CCPA. This statement serves the important purpose of signaling the Agency’s intent to take a reasonable approach to enforcement of certain provisions to account for the potential lack of preparation time that companies may have between the issuance of the final regulations and the law’s effective date.

However, this raises the issue of how, prior to an investigation being initiated, businesses might provide the relevant facts or information, such as regarding their good faith efforts to comply, for the Agency to consider in exercising its discretion to initiate investigations. Furthermore, at the point when the regulations specify that businesses present their information and arguments for consideration - in the probable cause hearing described in §7302 - it does not appear that the Agency has the same discretion to consider things like a business's "good faith efforts to comply," as §7302(a) specifies merely that "probable cause exists when the evidence supports a reasonable belief that the CCPA has been violated" and makes no mention of the discretionary considerations provided in §7301(b).

Therefore, §7301(b) of the regulations should specify an appropriate forum or other specific way(s) for businesses to submit relevant facts to the Agency, such as regarding any "good faith efforts to comply," for the Agency to consider before it makes its decision to pursue an investigation (and/or indicate whether the same discretion the Agency has in Regulations §7301(b) would apply in its determination of whether there is probable cause).

### **3. Recommended Revisions to Regulations Section 7301(b)**

In order to clarify the Agency's discretion in initiating investigations, we recommend modifying §7301(b) to clarify how and when businesses could submit information, prior to the probable cause hearing, for the Agency to consider in its determination whether to initiate an investigation. Alternatively, the regulations could extend the same discretion that the Agency has in §7301(b) to §7302(c)(2) by adding the language from §7301(b) to the end of §7302(c)(2) as well.

## **D. PROPOSED REGULATIONS SECTION 7001(p) AND 7050(g): DEFINITION OF "NONBUSINESS"; SERVICE PROVIDERS AND CONTRACTORS**

### **1. Summary of Comment**

The example and reasoning given in the definition of "Nonbusiness" in section 7001(p) of the Regulations is inconsistent with the CCPA's definition of a "business". Cal. Civ. Code § 1798.140(d). More broadly, circular reference left in section 7050(g) underscores a need for the Agency to clarify the definition of a "business" under the CCPA in the Regulations.

## 2. Substantive Reasoning for Recommended Revisions

### a. Consistency

The OAL's standard of review provides that a regulation is consistent when it is "in harmony with, and not in conflict with or contradictory to [the law]." Cal Gov. Code §11349(d).

The Regulations define "Nonbusiness" as:

"[A] person or entity that does not meet the definition of a 'business' as defined in Civil Code section 1798.140, subdivision (d). For example, non-profits and government entities are Nonbusinesses because "business" is defined, among other things, to include only entities 'organized or operated for the profit or financial benefit of its shareholders or other owners.'" Regulation §7001(p).

Civil Code Section 1798.140(d)(2) states that "any entity" can be a business that "controls or is controlled by a business ... and that shares common branding with the business and with whom the business shares consumers' personal information." In addition, Civil Code Section 1798.140(d)(4) provides that a "business" can be any "person that ... voluntarily certifies to the California Privacy Protection Agency that it is in compliance with, and agrees to be bound by, this title."

The example given in Regulation §7001(p) specifies that non-profits and government entities are examples of "Nonbusinesses" because a business is required to operate for profit. Non-profits could, however, fall under the definition of a "business" according to CCPA §1798.140(d)(2), because non-profits can meet all the elements of a "business" under that section: non-profits could control or be controlled by a "business", share common branding with a "business" and receive consumer personal information shared from a "business." Non-profits could also meet the conditions of §1798.140(d)(4) if they voluntarily certified their compliance with the CCPA. Neither §1798.140(d)(2) nor §1798.140(d)(4) of the CCPA requires that the entity in question must be "organized or operated for the profit or financial benefit of its shareholders or other owners" in order to be considered a "business."

Therefore, the example and reasoning given in the definition of "Nonbusiness" provided in Regulation §7001(p) is inconsistent with the statutory language of the CCPA and serves to confuse rather than clarify the interpretation of the statute.

### b. Clarity

The Agency's general mandate is to implement regulations that are necessary to effectuate the CPRA and clarify its interpretation. Moreover, regulations themselves must meet the OAL standard of clarity, meaning "written or displayed so that the meaning of regulations will be easily understood by those persons directly affected by them." Cal. Gov. Code 11349(c).

Given the removal of its long example, Regulation §7050(g), as written, merely refers back to meeting the CCPA's definition of a "business" as the determining factor in "[w]hether an entity that provides services to a Nonbusiness must comply with a consumer's CCPA request," as does the meaning of the new term "Nonbusiness." However, instead of adding clarity, this reference instead highlights significant ambiguities in the CCPA's definition of "business" that the Agency should address in the Regulations.

Although several CCPA obligations depend on whether or not an entity or person is a "business," the Regulations do not further clarify how an entity can determine it is a "business" for the purposes of §7050(g) or any other section and the determination of whether an entity is or is not a "business," is not necessarily easy to determine by the factors set forth in the CCPA statute itself.

For example, CCPA §1798.140(1)(A) provides that one of the thresholds for a "business" is "annual gross revenues in excess of twenty-five million dollars." Global organizations that do business in California may exceed this threshold if the calculation of annual gross revenue includes worldwide revenue, but not meet it if the threshold depends only on California revenue. Thus, it is unclear if the threshold in §1798.140(1)(A) means annual global revenue or annual revenue from operations in the State of California alone.

Furthermore, in sections 1798.140(d)(2)-(3), the word "shares" appears several times throughout. It is unclear if any or all uses of the word "shares" in these sections should be interpreted using the common understanding of that word or interpreted as the CCPA itself defines the term "share": "sharing ... a consumer's personal information by the business to a third party for cross-context behavioral advertising." *Id* at 140(ah)(1).

Finally, §1798.140(d)(4) provides that a "business" can be any "person that ... voluntarily certifies to the California Privacy Protection Agency that it is in compliance with, and agrees to

be bound by, this title.” The manner or mechanism by which a person may voluntarily certify to the Agency, and/or the standard for the actions, statements, or representations that might qualify as voluntary certification, is ambiguous and not clarified in the Regulations.

We believe these ambiguities demonstrate the need for the Agency to clarify the scope and meaning of “business” throughout the Regulations, including in §7050(g), in addition to trying to define what is a “nonbusiness.” The definition of a “business” is even more central to an organization’s CCPA compliance obligations, and the Regulations should facilitate compliance by clarifying and resolving these ambiguities.

### **3. Recommended Revisions to Regulations Section 7001(p) and 7050(g)**

We recommend removing the example and reasoning in regulation §7001(p)’s definition of the term “Nonbusiness” in its entirety because it is inconsistent with the CCPA and thus adds confusion rather than clarity to the statutory interpretation. The Agency must also use the Regulations to further clarify the definition of “business,” with a focus on the ambiguities identified above.

## **E. PROPOSED REGULATIONS SECTION 7025(c): OPT-OUT PREFERENCE SIGNALS**

### **1. Summary of Comment**

Regulation §7025(c) is inconsistent with the CCPA because it extends the consumer’s right to opt-out of the sale or sharing of personal information to “pseudonymized” information,” which, by its definition, would impermissibly require a business to re-link the pseudonymized information with additional information so as to render it attributable to a particular consumer or device in order to operationalize the opt-out. In addition, this requirement could disincentivize businesses from implementing pseudonymization as a privacy protection tool.

### **2. Substantive Reasoning for Recommended Revisions**

The CCPA’s definition of personal information includes “the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household: Identifiers such as ... unique personal identifiers ...” Cal. Civ. Code §1798.140(v)(1)(A), where the term “unique personal identifier” means a “persistent identifier that can be used to recognize a consumer, a



family, or a device that is linked to a consumer or family ....” *Id* at 140(aj). A consumer’s right to opt-out of the sale or sharing of personal information under CCPA §1798.120 applies to personal information only.

As recently revised, Regulation §7025(c)(1) states that:

“[When a business that collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b):] the business shall treat the opt-out preference signal as a valid request to opt-out of sale/sharing submitted pursuant to Civil Code section 1798.120 for that browser or device and any consumer profile associated with that browser or device, including **pseudonymous profiles** [emphasis added].”

The CCPA separately defines the term pseudonymize or pseudonymization as “the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.” Cal. Civ. Code §1798.140(aa). Further, CCPA §1798.145(j) provides, in relevant part, “This title shall not be construed to require a business service provider, or contractor to: (1) Reidentify or otherwise link information that, in the ordinary course of business, is not maintained in a manner that would be considered personal information. . . (3) Maintain information in identifiable, linkable, or associable form, or collect, obtain, retain, or access any data or technology, in order to be capable of linking or associating a verifiable consumer request with personal information.

As the CCPA’s definition of pseudonymization explains, personal information that is pseudonymized (i.e., pseudonymous information) is “**no longer attributable** [emphasis added] to a specific consumer without the use of additional information.” Cal. Civ. Code §1798.140(aa). In other words, the act of pseudonymizing personal information severs the link, or attribution, between information and a specific consumer or device. Thus, a “pseudonymous profile” could not be a consumer profile associated with a particular browser or device from which an opt-out signal was received, at least not without requiring, contrary to §1798.145(j), that a business re-link the separate information to an identifier associated with a particular consumer or device solely for the purposes of effectuating an opt-out received via browser signal.

The recent addition to regulation §7025(c)(1) is inconsistent with §1798.120 and §1798.145 of the CCPA because it extends the obligation to effectuate an opt-out of sales and sharing to “pseudonymized profiles.” If the Agency does not modify section 7025(c), it will be inconsistent with the CCPA for the reasons explained above and effectively nullify pseudonymization under the CCPA. Pseudonymization can be a powerful privacy protection tool, but businesses would have almost no incentive to implement pseudonymization because it would have virtually no value for CCPA compliance.

### **3. Recommended Revisions to Regulations Section 7025**

The Agency should revert the changes to Regulation §7025(c)(1) and strike the illustrative example in §7025(c)(7) or revert to the initial proposed text (single blue underline). More generally, the Agency should encourage pseudonymization in the Regulations by specifying the procedures and standards for pseudonymization and providing examples or criteria to help organizations benefit from using the privacy protective tool of pseudonymization.

Respectfully submitted.

---

**From:** Jan Ortonowski | Preiskel & Co [REDACTED]  
**Sent:** Monday, November 21, 2022 10:35 AM  
**To:** Regulations  
**Cc:** Stephen Dnes | Preiskel & Co; Timothy Cowen | Preiskel & Co; Competition  
**Subject:** RE: CPPA Public Comment  
**Attachments:** 2022.11.21\_MOW's Comments on Proposed Regulations to Implement the Consumer Privacy Rights Act of 2020 (CPRA).pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear Sirs,

There was a typographical error contained in our earlier submission. Therefore, we have attached a corrected submission of our comments in response to the CPPA's proposed regulatory action. We kindly ask that the CPPA use this new version only.

Kind regards,

Jan Ortonowski

**Jan Ortonowski** | Competition Paralegal

**Stephen Dnes** | Senior Consultant | Preiskel & Co LLP

**PREISKEL & CO**

Preiskel & Co LLP, 4 King's Bench Walk, Temple, London EC4Y 7DL

t + [REDACTED]

[www.preiskel.com](http://www.preiskel.com)

---

**From:** Jan Ortonowski | Preiskel & Co  
**Sent:** 21 November 2022 11:14  
**To:** 'regulations@cpha.ca.gov' <regulations@cpha.ca.gov>  
**Cc:** Stephen Dnes | Preiskel & Co <[REDACTED]>; Timothy Cowen | Preiskel & Co <[REDACTED]>; Competition <[REDACTED]>  
**Subject:** CPPA Public Comment

Dear Sirs,

Please find attached comments in response to the CPPA's proposed regulatory action to implement the Consumer Privacy Rights Act of 2020 (CPRA) submitted on behalf of the Movement for an Open Web.

We appreciate your consideration of our feedback as your agency moves through the rulemaking process on this important issue. We are happy to answer any questions you may have and to discuss these issues in more detail.

Kind regards,

Jan Ortonowski

November 21, 2022

California Privacy Protection Agency  
Attn: Brian Soublet  
2101 Arena Blvd., Sacramento, CA 95834  
[regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

**Re: Comments on Proposed Regulations to Implement the Consumer Privacy Rights Act of 2020 (CPRA)**

Dear Mr. Soublet and Members of the California Privacy Protection Agency:

The Movement for an Open Web (“MOW”) welcomes the California Privacy Protection Agency’s efforts to provide improved clarity around how businesses may meet their obligations under California’s Privacy Act (“CPRA”). MOW is a coalition of publishers, broadcasters, advertising technology providers, and other stakeholders within digital ecosystems.

The following comments reflect MOW members’ perspectives on the most recent proposed regulations related to safeguarding people’s important privacy rights while also enabling responsible business-initiated data handling. While the comments below to newly revised text are brief, so as to focus on the highest priority issues, the lack of comment does not mean there are no additional points our members wish to raise with the proposed regulations.

Executive summary:

- Improving clarity of data protection regulations is important to remove uncertainty relating to supply chain partners (aka “third parties”) that most businesses rely upon in data driven markets.
- Retaining incentives to implement privacy-by-design safeguards, even absent intentional user choice signals, is an important policy matter to protect. This is especially so where users wish to interact with advertising supported digital properties and are not in a position to decide on business-to-business advertising system design choices, in which there may be no direct or even indirect consumer interest, as where there is no risk of harm. The key is to ensure reasonable consumer protection, not least when risk associated with the data required for such purposes is often (although not always) low.
- Relaxing the need to disclose at collection all the partners an organization may choose to work with in the future, is a welcome improvement in the most recent draft of proposed regulations. This avoids risks of overwhelming consumers and allows business to business interoperability.

We wish to highlight that smaller organizations necessarily rely on more supply chain partners to operate and grow than the larger organizations with which they compete. As a consequence of their size they cannot rely on in-house solutions, and instead buy equivalent services from their vendor partners. For these organizations, competition among such business solutions is therefore vital, and undue restrictions on supply chain choice and interoperability can harm content production by damaging competition in the supply chain, ultimately harming content producers and the choices available to consumers. Protecting interoperability and the ability to undertake responsible exchanges of information among businesses is thus very important to ensuring that consumers can continue to benefit from a diversity of niche digital content and services, which more often serves underrepresented minority interests than their larger, vertically-integrated rivals.

Many organisations are now facing increasing uncertainty around how they can continue to operate and compete against these larger organizations because of ambiguities in some recent data protection regulations, which constrain the ability to use supply chain partners (aka “third-parties”) even in cases where risks to individuals are low. This uncertainty results from difficulties from limitations in guidance as to required reasonable risk mitigation measures. Greater clarity about the reasonable measures organisations can put in place will help to balance the important privacy rights of individuals with organisational needs for the responsible use of data. This will make it easier for organisations of all sizes to continue to innovate, operate and grow in today’s data-driven world. Alternately, policies that exempt first parties from identical obligations as required for supply chain supported businesses will merely centralize more data and power into the hands of the largest digital platforms and internet gatekeepers, ultimately reducing transparency, choice and control for consumers on how and from whom they may access digital content and services.

### **Ensure organisations continue to be incentivised to implement privacy-by-design safeguards**

Data protection regulations incentivise organizations to put in place privacy-by-design safeguards designed to protect specific individual’s personal data, such as pseudonymization. This is a critically important policy that ensures businesses minimize the use cases that rely on information linked to specific individuals or households, by adopting safeguards to ensure that high standards of privacy protection are met.

Safeguards should be assessed in relation to relative risks. Not all data use poses equal risks, and organizations should be incentivized to continue to rely on lower-risk use cases that collect and process data not linked to specific individuals (e.g., frequency capping, fraud detection, attribution and billing purposes). In such cases, a range of sensible and business-appropriate safeguards (e.g., pseudonymization) would be apt. Other safeguards include appropriate privacy-by-design measures such as contractual restrictions to further reduce risk (such as mentioned in CPRA’s definition of “pseudonymization”). The guiding aim should be to encourage business to adopt reasonable risk mitigations, rather than shift data handling only to larger organizations which escape obligations under the current law due to the existing first-party exemptions inherent in focusing only on “cross-context” behavioural advertising.

In places, the most recent draft seems, perhaps inadvertently, to reduce such incentives by assuming appropriately pseudonymized data poses identical risks to individuals as when using their directly-identifiable identity. This will often be untrue, notably in low-risk cases where pseudonymization is an adequate safeguard (e.g., a browser is shown an Open Web campaign-level frequency-capped sports advert based on current sports website context).

For example, new language in § 7025 (c)(2) as currently drafted could be read to encompass even those cases where an organisation *does not* collect a specific identity information about an individual or household’s identity:

*For example, a business may give the consumer the option to provide information that identifies the consumer so that the request to opt-out of sale/sharing can apply to offline sale or sharing of personal information. However, if the consumer does not respond, the business shall still process the opt-out preference signal as a valid request to opt-out of sale/sharing for that browser or device and any consumer profile the business associates with that browser or device, including pseudonymous profiles. (emphasis added)*

Privacy-by-design measures mean that data linked to the identity of a specific individual or household is protected just as much as data never or no longer linked, provided that robust safeguards are in place. This should be captured in the provision. This tension can also be seen in conflict with the example in § 7025 (c)(7)(D). This example speaks to conflicting consumer preferences where safeguards are in place:

*(D) Ramona participates in Business P's financial incentive program where she receives coupons in exchange for allowing the business to pseudonymously track and share her online browsing habits to marketing partners. Ramona enables an opt-out preference signal on her browser and then visits Business P's website. Business P knows that it is Ramona through a cookie that has been placed on her browser, but also detects the opt-out preference signal. Business P may ignore the opt-out preference signal, but must and notify Ramona that her opt-out preference signal conflicts with her participation in the financial incentive program and ask whether she intends to withdraw from the financial incentive program. If Ramona does not affirm her intent to withdraw, **Business P may ignore the opt-out preference signal** and place Ramona on a whitelist so that Business P does not have to notify Ramona of the conflict again.*

The position is correct from the consumer point of view, as the more consumer-friendly benefit is retained over the conflicting no-processing preference collected in a different context. This aligns with the consumer's expressly stated preference, which is to receive the discount, and as no question is asked as to whether the data processing should take place *in the context of the loss of the coupons* it is sensible to allow continued processing, so long as appropriate safeguards are in place. As the data use is pseudonymized, and the data use consumer-friendly, avoiding overbroad interpretation of opt-outs is helpful.

So, the presumed conflict may be resolved by assuming that processing in § 7025 (c)(2) only applies to cases where the business (or any of its partners) link the specific individual's data to their identity (in this particular case Ramona). It would be helpful to conform other references to pseudonymization to this sensibly pragmatic approach.

### **Ensuring required disclosures do not overwhelm consumers**

It is often said that sunlight is the best disinfectant. However, too much light can be blinding. Seen from this view, overwhelming consumers with information that is not meaningful does not advance any data protection goals that the legislature set out. In fact, burdensome disclosures can harm data protection because it is then difficult for consumers to notice much less control the more concerning higher-risk data processing cases.

Accordingly, we were pleased to read the revisions that removed the disclosure requirements of third parties to which a covered business may in the future share with the supply chain partners most businesses must rely upon in Disclosure Requirements § 7012 (e)(6). Providing to consumers long lists of all supply chain partners an organisation may choose to work with in the future would overwhelm consumers and fail to meaningfully inform them of any criteria that may increase or decrease risks associated with the collection and processing of their Personal Data. It is also important that future businesses and future use cases remain open, so long as safeguards are in place and consumers are not harmed, as this allows future innovative new entrants as well as new uses while still ensuring strong data protection.

### **Accounting for very large online platforms and potential distortions to competition**

The top four to five largest technology platforms have over a billion end users across the globe. Almost all Californian residents use their services. They have scale, scope, and other economic advantages over many thousands of smaller rivals. They have a direct interface with end users that smaller rivals often do not. Thus, making privacy laws subject only to end user consent risks reinforces the market power of the largest rivals, and can harm competition.

Smaller rivals rely on the ability to engage supply chain partners or simply to operate at different levels in supply chains at which obtaining individual consent may prove difficult or impossible. Pseudonymization that generates de-identified data is a very important compliance mechanism for such use cases and its status as a valid compliance mechanism in low risk contexts is particularly important.

### **Concluding remarks**

Data protection regulations should be easy for all organizations to comply with and should not discriminate against smaller businesses. This is especially important in troubling economic and social times, which many are experiencing. Data-driven innovation and solutions have fuelled California's growth and indeed that of many around the globe bettering the lives of billions, especially through the provision of ad-funded content which is particularly relied upon by the less financially well off. It will be important to avoid inadvertently distorting competition in efforts to improve the digital economy for all people. Thus, we continue to welcome constructive guidance that helps organizations continue to operate responsibly, balancing their own interests and those of service users with safeguarding people's important privacy rights. The key to addressing this trade-off well from a societal point of view is to take a reasonable risk-based approach to appropriate safeguards, rather than to aim to limit all data processing for only smaller organizations.

We appreciate your consideration of our feedback as your agency moves through the rulemaking process on this important issue. We are happy to answer any questions you may have and to discuss these issues in more detail.

Sincerely,

Movement for an Open Web

---

**From:** Alvaro Marañon [REDACTED]  
**Sent:** Monday, November 21, 2022 5:24 AM  
**To:** Regulations  
**Cc:** Stephanie Joyce  
**Subject:** Re: CPPA Public Comment  
**Attachments:** 2022-11-21\_CCIA Comments to CPPA on Modifications to Draft Regulations.pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

To California Privacy Protection Agency,

The Computer & Communications Industry Association (CCIA) is pleased to provide input on the proposed modifications to the draft regulations under the California Consumer Privacy Rights Act.

We appreciate your consideration of the comments included in the attached file.

Thank you,

Alvaro Maranon  
Policy Counsel  
Computer & Communications Industry Association (CCIA)  
[REDACTED]

@CCIANet





November 21, 2022

**Via Electronic Mail (regulations@coppa.ca.gov)**

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

**Re: CPPA Public Comment**

The Computer & Communications Industry Association (“CCIA”)<sup>1</sup> is pleased to respond to the California Privacy Protection Agency (the “Agency” or “CPPA”) [Notice of Modifications](#) to the Proposed Regulations (the “Regulations”) that will implement the California Privacy Act of 2020 (the “CPRA”).

**INTRODUCTION**

CCIA has long supported the evolution of privacy policy to keep pace with evolving technologies. We support and appreciate the Agency’s efforts to adopt and implement privacy regulations that will guide businesses and protect consumers. The Regulations are an impressively comprehensive set of protections and are, by far, the most developed guidelines in the nation.

These comments focus on the provisions in the proposed modifications to the Regulations (“Modified Draft Rules”) that warrant revision. The aim of these suggestions is manifold. First, to ensure that the Regulations are reflective of the mandates stated in the CPRA. Secondly, the Regulations are feasible to implement in a timely and clear manner. And third, the Regulations allow flexibility in order not to inhibit innovation, which would lead to harm to businesses and consumers.

CCIA’s suggested amendments to the Regulations are set forth in **Attachment A**.

---

<sup>1</sup> CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms. For 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than \$100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at <https://www.ccianet.org/members>.

## I. GENERAL PROVISIONS

### A. **Restrictions on the Collection and Use of Personal Information – § 7002**

The proposed modifications to § 7002 create overly prescriptive requirements that conflict with the intent of the CPRA. As highlighted by the California Privacy Protection Agency Board (the “Board”) during its October meetings, the CPRA intended for this provision to provide guidance on how the requirements for this section should be understood by businesses and consumers. Purpose limitation, data minimization, and robust principles for data governance are critical and foundational elements of comprehensive privacy and data regulation. The Regulations should incorporate reasonable and proportionate standards to craft principles that balance innovation and consumer privacy.

However, the Modified Draft Rules neglect these considerations by proposing a complicated and subjective multi-factor balancing test that would apply to all collection, use, retention, and/or sharing of personal information. The highly open-ended nature of these requirements would place businesses in a constant state of uncertainty regarding whether they comply. Consumers could suffer given that a highly complex and open-ended framework would leave them with a lack of clarity regarding expectations for how their personal information will be collected, used, retained, or shared. CCIA recommends the Agency delete this multi-factor balancing test from the Regulations.

The overly narrow language in the illustrative examples could inhibit innovation. The proposed language in § 7002(b)(1) concerning the mobile flashlight application makes it clear that it should only provide flashlight services and not offer ancillary benefits that might rely on collected data—such as identifying restaurants that are too dimly lit or public areas with insufficient street lighting. This assumption—the primary function of a service should be the exclusive function—is narrower than the General Data Protection Regulation (GDPR) data minimization provision, which allows businesses to process personal information in ways that are adequate and relevant to what is necessary concerning to the purposes for which it is processed.<sup>2</sup> CCIA suggests the Agency clarify this language and include an example where the use of data to improve and build new features is not incompatible with the original purpose.

---

<sup>2</sup>See Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and

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. Consumers obtain substantial benefits from sharing data across services, such as using data from a reading app to personalize book recommendations in an online store (whether both services are offered by the same business). To avoid consumers missing from these benefits, CCIA suggests the Agency modify this consideration to clarify whether the business' use of the collected information on a different product or service is unexpected and unrelated.

Marketing and other non-privacy disclosures should not be a guiding principle 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. Conversely, marketing materials highlight the benefits of the product or service and are not necessarily relevant to how data is used, unless the disclosure makes that connection explicit. CCIA recommends the Agency remove the marketing language in § 7002(b)(4) from the Regulations.

The proposed language in § 7002(b)(5) does not offer sufficient guidance for assessing a consumer's reasonable expectation. Consumers often lack the necessary business background to understand processor relationships or the context to reflect on how a business processes its data. To the extent this guiding principle on the degree of involvement is retained, the Regulations should be modified to focus on uses that are unexpected and offensive concerning disclosed uses.

#### **B. Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent – § 7004**

When designing consumer requests and obtaining consent, businesses should be required to ensure that the language is easy to understand, that there is no manipulative or confusing language, that there is symmetry in choice, and that the methods present “easy-to-execute” options. The Regulations appropriately state that non-compliant design methods may be considered dark patterns that do not result in valid consent. But the Modified Draft Rules go beyond the CPRA and create subjective inquiries that make it difficult to operationalize for

---

Repealing Directive 95/46/EC (General Data Protection Regulation), art. 5(c), (“Principles Relating to Processing of Personal Data”) 2016 O.J. (L 119) 38 (EU) [hereinafter GDPR].

businesses. For example, the revised provision still places an undue burden on design through requirements on exact symmetry in length, which might not be appropriate in all instances, and to avoid “disruptive screens.” One of the key principles for consumer consent is that they are informed of their decision. Businesses should be able to inform a Consumer about the effects of their choice without it constituting a disruption or rising to the level of a dark pattern. CCIA recommends the Agency modify the Regulations to focus on prohibiting false or misleading language that could impair or interfere with a consumer's ability to exercise their choice.

## **II. REQUIRED DISCLOSURES TO CONSUMERS**

### **A. Notice at Collection of Personal Information – § 7012**

The Modified draft rules on third-party data collection requirements in § 7012(g)(2) are overly prescriptive for companies. Businesses often engage with various third parties for numerous services that may involve the collection of data but the focus on a physical display is disproportionate, creating an unnecessary mandate to display a physical notice despite other methods being more effective and in turn, beneficial for a consumer. For instance, if a store or restaurant employs a third-party voice assistant device that does not contain a physical display, then a notice directing the consumer to the third-party device’s website should be sufficient. The Agency can look to the Federal Trade Commission (FTC) which has provided guidance for providing appropriate disclosures in various contexts through its *Dot Com Disclosures* – clarified that ensuring clear disclosure of appropriate terms based on text and available means is the more important standard upon which to rely. The FTC has made clear that using email instead of direct mail may be appropriate as long as a website operator discloses how it will provide information and provides it in a form that consumers can retain. This approach demonstrates an understanding of the need for flexibility and adaptability in creating a meaningful user experience.

The Regulations should follow a similar approach and permit notice that is “reasonable” in the context of the method of data collection. CCIA recommends the Agency modify § 7012(g)(2) to adopt the flexibility permitted by the FTC, which will enable businesses to better engage with service providers and still allow meaningful disclosures to consumers.

### **B. Notice of Right to Opt-Out of Sale Personal Information – § 7013**

CCIA is concerned that modifications to § 7013(e)(3) exceeds the mandate of the CPRA.

This proposed modification would expand notice obligations by requiring businesses to offer an opt-out in the same manner as it discloses how data is collected, imposing heavy burdens on businesses that maintain a website but collect personal information by other means. But the CPRA only requires that the business disclose the consumer's right in its online privacy policy or on the Internet webpage.<sup>3</sup> The Agency has explained that the requirement seeks to address new ways in which businesses are collecting personal information and ensure that the notice is effective.<sup>4</sup> However, the proposed modifications would increase the burden upon businesses by no longer permitting a brick-and-mortar store to post signage directing consumers to an online notice or require a business collecting personal information over the phone to "orally" walk through the notice. In these settings, the business should have the option of "orally" directing the consumer to the website notice, as permitted for physical stores.

By way of comparison, the Virginia Consumer Data Protection Act (VCDPA) and Colorado Privacy Act (CPA) only require businesses to present opt-out methods clearly and conspicuously in privacy notices and readily accessible locations outside of privacy notices. These opt-outs are not required to be presented in the same manner as data collection. Adopting the approach taken in other state privacy laws, by contrast, will be beneficial to businesses and consumers as there is a clearer path forward regarding how best to provide and act upon consumer rights. A business that collects personal information outside a website should be able to satisfy its obligation by directing the consumer to its website. CCIA suggests the Agency modify the Regulation to be consistent with what is becoming the national approach and what is required by the CPRA.

The proposed modifications in § 7013(h) do not provide sufficient language specifying when the requirement to obtain opt-out consent for pre-data collection applies. The Regulations need to ensure businesses and consumers understand that the requirement will apply to data collected after the notice requirement goes into effect. CCIA recommends the Agency modify the Regulation to require affirmative consent to sell/share information collected before the opt-out notice but limiting it to information collected after the notice requirement goes into effect. These temporal specifications will align with the Regulations of privacy laws in other states,

---

<sup>3</sup> 6 CAL. CONSUMER PRIVACY ACT REGULATIONS, § 11 CCR 7021(a) (2022) § 1798.130(a)(5) [CPRA]

<sup>4</sup> See Cal. Privacy Protection Agency, Initial Statement of Reasons (Jun. 6, 2022), [https://cppa.ca.gov/meetings/materials/20220608\\_item3\\_isr.pdf](https://cppa.ca.gov/meetings/materials/20220608_item3_isr.pdf).

which do not prevent businesses from engaging in targeted advertising based on information already collected.

### **C. Alternative Opt-Out Links – § 7015**

Modified Draft Rule § 7015(b) would mandate that businesses provide the opt-out icon despite it being optional under the CPRA. This new requirement may confuse consumers given that the static image looks like a toggle that a consumer can activate. This requirement also prescribes a graphic feature that may not align with a business' design layout, putting an unnecessary burden on a business without countervailing consumer benefit. CCIA recommends the Regulations do not include this requirement for an opt-out icon.

## **III. BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS**

### **A. Request to Delete – § 7022**

CCIA suggests that Agency modify § 7022(c)(4) to require “reasonable efforts” to notify third parties when the deletion is made. This would help alleviate businesses from the potential flood of requests that may come in, this delimiter would help businesses meet this requirement and, in the end, benefit the consumers.

### **B. Request to Correct – § 7023**

The Modified Draft Rules would require a business to comply with a consumer's request to correct without any limitation. The lack of any delimiter could make this obligation overly burdensome for businesses. CCIA recommends the Agency add a “disproportionate effort” standard. This modification would prevent businesses from exerting disproportionate effort in meeting correction requests and comport with other state privacy laws that allow businesses an exemption from fulfilling requests for correction where it would be unreasonably burdensome for the controller to associate the request with personal information.<sup>5</sup>

### **C. Opt-Out Preference Signals – § 7025**

---

<sup>5</sup> See VA. CONSUMER DATA PROT. ACT, H 2307, 2021 SPECIAL SESSION, § 59.1-577 (2022); see also COL. PRIVACY ACT, SB 21-190, 2021 REG. SESS., § 6-1-1307 (2022); CT. ACT CONCERNING PERSONAL DATA PRIVACY AND ONLINE MONITORING, PA 22-15, 2022 Gen. Assemb., § 9(c) (2022).

By requiring that businesses recognize global opt-out preference signals, the proposed language in § 7025(b) goes beyond and contradicts what is stated in the CPRA. Section 1798.135 of the statute makes clear that businesses may choose to either provide links for consumers to opt-out of “selling,” “sharing,” or certain uses and disclosures of sensitive personal information; or recognize universal opt-out preference signals. Specifically, the inclusion of “if” in the CPRA reflects the clear intent that the recognition of global opt-out preference signals is to be voluntary.<sup>6</sup> The statute reinforces this intent in the subsequent provision through the inclusion of *allows* – “A business that *allows* consumers to opt out of the sale or sharing of their personal information and to limit the use of their sensitive personal information under paragraph (1) . . . ”<sup>7</sup>

The Modified Draft Rules, by contrast, reject this distinction. The CPRA recognized the importance of providing businesses with this flexibility given the many uncertainties that remain concerning how such signals would be implemented, how businesses are to treat multiple global opt-out preference signals that could conflict, and how to ensure that such signals do not have anti-competitive consequences. CCIA recommends modifying Section 7025(b) to ensure the recognition of global opt-out preference signals is voluntary, to align with the CPRA. These changes should be applied throughout § 7025 to reflect that recognition of global opt-out preference signals is voluntary.

In addition, CCIA suggests that the Regulations should permit consumers to turn on and turn off the opt-out mechanism discussed in § 7025(b). The opt-out mechanism should also harmonize the treatment of that signal with the confirmatory display discussed in § 7026(g). These provisions would make the signal more user-friendly, which is a stated goal of these Regulations as indicated in § 7025(a). They would also be consistent with the treatment of cookie settings (which encompasses signals such as this) under the GDPR and Europe’s ePrivacy Directive, which provide clarity that: (1) a business’s website should feature a consent banner that allows visitors to either give or refuse consent to the non-necessary cookies that process personal information; and (2) methods for offering a right to refuse or requesting consent should be made as user-friendly as possible, and settings should remain available for users to revisit and

---

<sup>6</sup> “A business shall not be required to comply with subdivision (a) if the business allows consumers to opt out of the sale or sharing of their personal information and to limit the use of their sensitive personal information through an opt-out preference signal. . . .” CPRA, § 1798.135(b)(1)

<sup>7</sup> CPRA, § 1798.135(b)(2)

adjust, as they prefer.<sup>8</sup> Consistent treatment of signals and settings assists businesses with compliance by creating a unified, global approach.

CCIA is concerned about the scope of the requirements for businesses to process a universal opt-out mechanism (“UOOMs”). Specifically, CCIA recommends that the Agency confirm the requirements to honor UOOMs should not exceed the capabilities of eligible UOOMs that are available in the marketplace. For example, if only browser extensions can serve as UOOMs, the requirement to honor UOOM signals should only extend to browsers.

The illustrative example in §7025(c)(7)(A) appears to create unnecessary risk to consumers’ privacy. The proposed language may require businesses to take extra action to associate an unauthenticated visitor with an account, which is less privacy-friendly. CCIA recommends the Regulations be modified to focus on whether the visitor is logged in to avoid any obligation for a company to process additional personal data.

#### **D. Request to Opt-Out – § 7026**

The Modified Draft Rules conflict with the statute by expanding what businesses should consider when determining the methods consumers may use to submit requests to opt-out. Instead of being limited to what is sold or shared, the Agency expands the consideration to personal information that the business “makes available to third parties.” It is unclear why the Agency seeks to expand this scope, which is not aligned with Section 1798.100(d) of the statute nor consistent with the other proposed changes to the Regulations. Moreover, the modifications would add a new limitation for processing in a frictionless manner. CCIA recommends the Agency remove the added limitation for processing in a frictionless manner, especially given that the alternatives and the benefits to the consumer are unclear.

The requirement to notify third parties of a consumer’s opt-out status should apply on a going-forward basis only; it should not require a company to go back to previous transactions by sending the opt-out request to all downstream partners. In any case, the notification requirement should (1) be limited only to the third parties to whom the business has sold or shared the customer’s personal information, as opposed to § 7026(f)(3)’s requirement to notify all third parties with whom the business makes personal information available; and (2) include the

---

<sup>8</sup> See OFFICIAL JOURNAL OF THE EUROPEAN UNION, DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 25 NOVEMBER 2009, SECTION 20(a).



disproportionate effort standard, to prevent a business from expending unnecessary time and resources with little benefit to consumers. Indeed, while the GDPR does require notice to third parties when a consumer exercises their rights, it does not require such notice if it would require the business to expend disproportionate effort. CCIA recommends deleting §7026(f)(2).

#### **IV. SERVICE PROVIDERS, CONTRACTORS, AND THIRD PARTIES**

##### **A. Service Providers – § 7050**

The illustrative example in § 7050(b)(1) of the Modified Draft Rules purports to prohibit a form of widely accepted advertising based on email addresses. The statute permits these established practices while the basis for this proposed modification is unclear. The example would have significant implications for businesses, especially small businesses, that rely on these advertising tools to reach their customers with information that is provided to them for this purpose. A customer list that a business uploads, provided they have the necessary permission to do so and it is hashed, helps them effectively and efficiently reach their customers in a privacy-protective manner. Restricting the ability for California businesses to use such tools will make it more difficult for them to reach their customers on social media platforms, increase the costs for advertising, and disproportionately affect their ability to compete in the U.S., and global, digital markets. Especially against those competitors who operate outside the scope of the statute. CCIA's proposed modifications in Attachment A would align the example with the statute, drawing directly from the statute's definition of cross-context behavioral advertising, and avoids creating further uncertainty for businesses.

Modified Draft Rule § 7050(e) would convert all service provider or contractor relationships into third-party relationships, with a host of additional legal obligations, where the contract is not fully compliant with the Regulations. This proposal would create a disproportionate and compounding penalty when a business fails to have the required contract in place. Designating a service provider as a third party would not accurately reflect the business relationship and imposes compounding penalties by also likely necessitating a violation of the sale opt-out (which would not apply to service provider relationships). Moreover, the triggered third-party classification would not reflect the actual relationship between the business and the external party, which might be engaged in an otherwise permitted business purpose that is neither selling nor sharing. The violation of the contract provision, standing alone, would be a sufficient penalty. CCIA advises the Agency to delete this provision.

**B. Contract Requirements for Service Providers and Contractors – § 7051**

Section 1798.145 of the CPRA includes an exemption that exculpates businesses from a service provider and contractor non-compliance where appropriate due diligence has been conducted. CCIA encourages the Agency to provide clarity by listing factors that affirmatively indicate a violation instead of leaving businesses to formulate a reasonable belief that the external party is in violation. By listing affirmative factors, the Regulations will not place additional burdens on businesses to confirm the absence of violations. Rather, businesses will be equipped with guidance on how to best conduct due diligence, which is similar to the guidance provided to data exporters in the European Commission’s Standard Contractual Clauses (SCCs). Just as the SCCs offer guidance to data exporters by instructing them that they may, “take into account relevant certifications held by the data importer” when deciding on a review or audit, the Regulations can and should also offer more clarity to businesses in this section.<sup>9</sup>

The language in § 7051(c) is also problematic for it creates a potential backdoor requirement that a business must conduct due diligence and audits on its service providers, contractors, and third parties. To the extent the Agency promulgates Regulations on when the exemption in section 1798.145(i) of the statute applies, they should be limited to factors that affirmatively indicate that the external party is violating its obligations – and not impose additional burdens on business to confirm the absence of violations. CCIA’s suggestions in Attachment A attempt to avoid creating this risk to businesses.

**C. Contract Requirements Third Parties – § 7053**

The proposed requirements for this provision also create the same risks as those identified in §7051(c). CCIA suggests updating § 7053(b) to address the same aforementioned concerns and incorporate specific factors to indicate a violation instead of leaving businesses to formulate a reasonable belief that the external party is in violation.

---

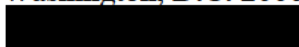
<sup>9</sup> European Commission, Annex to The Commission Implementing Decision on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679, Module 2 (8.9)(C), Transfer Controller to Processor: Documentation and Compliance, <https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clausescontrollers-and-processors>,

### CONCLUSION

CCIA and its members thank the Agency for this opportunity to provide suggestions on how to perfect the Regulations in ways that protect consumer data, are feasible to implement, and retain flexibility for customization and innovation. The suggested alternative language discussed herein, which is also provided in **Attachment A** in redline form for ease of review, is offered as a means for achieving the best result for consumers, regulators, and the online ecosystem.

Respectfully submitted,

Alvaro Marañon  
Policy Counsel  
Computer & Communications Industry Association  
25 Massachusetts Avenue, NW, Suite 300C  
Washington, D.C. 20001



November 21, 2022

## ATTACHMENT A

### Suggested Amendments to Proposed Rules

§ 7002(b)(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 an **unexpected and unrelated use on a** different product or service offered by the business or the business’s subsidiary.

§ 7002(b)(4): The specificity, explicitness, prominence, and clarity of disclosures to the consumer(s) about the purpose for collecting or processing their personal information, ~~such as in the Notice at Collection and in the marketing materials to the consumer(s) 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 their phone number for the purpose of verifying the consumer’s identity and not for marketing purposes. ~~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): The degree to which the involvement of service providers, contractors, third parties, or other entities in the collecting or processing of personal information **would be unexpected and offensive** ~~is apparent~~ to the consumer(s). 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.

§ 7004(a)(2): Symmetry in choice. 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 **to the extent** it impairs or interferes with the consumer’s ability to make a choice. Illustrative examples follow.

§ 7015(b): A business that chooses to use an Alternative Opt-out Link **may** ~~shall~~ title the link, “Your Privacy Choices” or “Your California Privacy Choices,” and shall include the following opt-out icon 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 other icons used by the business in the header or footer of its webpage.

§ 7025(b): A business that sells or shares personal information 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 or JavaScript object.
- (2) The signal shall have the capability to indicate that the consumer has selected to turn off the opt-out preference signal.
- (3) ~~(2)~~ 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): 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. 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.

§ 7026(a)(1): 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.~~

§ 7050(b)(1): Business S, a clothing company, hires a social media company as a service provider for the purpose of providing Business S's advertisements on the social media company's platform. The social media company can serve Business S by providing non-personalized advertising services on its platform based on aggregated or demographic information (e.g., advertisements to women, 18-30 years old, that live in Los Angeles). ~~The~~

social media company can also use a hashed customer list provided by Business S to serve Business S's advertisements to Business S's customers. However, it cannot use a list of customer email addresses provided by Business S to then target those customers with advertisements based on information obtained from other third party businesses's websites, applications, or services. ~~to identify users on the social media company's platform to serve advertisements to them.~~

~~§ 7050(e): A person who does not have a contract that complies with section 7051, subsection (a), is not a service provider or a contractor under the CCPA. For example, a business's disclosure of personal information to a person who does not have a contract that complies with section 7051, subsection (a) may be considered a sale or sharing of personal information for which the business must provide the consumer with the right to opt out of sale/sharing.~~

§ 7051(c): Whether a business conducts due diligence of its service providers and contractors factors into whether the business has reason to believe that a service provider or contractor is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract **where the business knows or has reason to believe that a violation of the CCPA and these regulations occurred** nor exercises its rights to **assess**, audit, or test the service provider's or contractor's systems might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the service provider or contractor.

§ 7053(b): Whether a business conducts due diligence of the third party factors into whether the business has reason to believe that the third party is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract **where the business knows or has reason to believe that a violation of the CCPA and these regulations occurred** might not be able to rely on the defense that it did not have reason to believe that the third party intends to use the personal information in violation of the CCPA and these regulations at the time of the business disclosed the personal information to the third party.

---

**From:** Matthew Powers [REDACTED]  
**Sent:** Monday, November 21, 2022 5:25 AM  
**To:** Regulations  
**Cc:** John W. Mangan; John Shirikian  
**Subject:** ACLHIC ACLI CPRA Modified Reg Text Comment Letter 11.21.22  
**Attachments:** ACLHIC ACLI CPRA Modified Reg Text Comment Letter 11.21.22 (Final).pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

To Whom It May Concern:

Please find attached a joint trades comment letter from the American Council of Life Insurers and the Association of California Life and Health Insurance Companies on the 11.3.22 CPRA Modified Regulations Text. We would be happy to answer any questions.

Sincerely,  
Matthew Powers

--

ACLHIC

P: [REDACTED]

[www.aclhic.com](http://www.aclhic.com)



November 21, 2022

Mr. Brian Soublet, Director  
 California Privacy Protection Agency  
 2101 Arena Blvd., Sacramento, CA 95834  
 Email: [regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

**Re: Comments on Modified Text of Proposed Regulations to Implement the Consumer Privacy Rights Act of 2020 (CPRA)**

Dear Director Soublet:

The American Council of Life Insurers (ACLI) and the Association of California Life and Health Insurance Companies (ACLHIC) respectfully submit the following comments on behalf of our members in response to your Modified Text of Proposed Regulations released November 3, 2022. We appreciate several changes that were made in line with suggestions from our August 23, 2022 letter, however we continue to have strong concerns with a number of areas of the proposed regulations, the lack of guidance in other areas and the accelerated compliance timeline that runs contrary to the intent of California voters when they passed Proposition 24.

As with our previous letter we begin with general comments about this rulemaking process and text, and then we highlight specific areas of concern within the language.

***General Comments:***

Building off the California Chamber of Commerce letter on November 3, 2022, which ACLHIC and ACLI co-signed, we continue to have very deep concerns that CPRA takes effect on January 1, 2023, yet there is still no finalized regulatory guidance with which insurers can build out their compliance systems. Through Proposition 24 voters made it clear that businesses would have 6 months between regulations being adopted and the law taking effect, and then a further 6 months until enforcement begins. With the current process this timeline is simply not being honored. Not only are the regulations going to be at least 5 months delayed, but the regulations do not capture critical areas where our members must have guidance: employee and business to business data, cybersecurity audits, risk assessments and automated decision systems. In effect we are going to be asked to comply with CPRA requirements without the necessary and required guidance from CPPA, and we believe this is both contrary to Proposition 24 and fundamentally unfair. Additionally, the January 1, 2023 lapse of the employee and business to business data sunsets creates further complications for compliance as these regulations do not account for this new, important and highly technical universe of data. This leaves open numerous areas where insurers will have to make good faith efforts to comply with the law without guidance of the agency as required by Proposition 24.

***Article 1: General Provisions***

**7001. Definitions**

(r): As noted in our previous letter, we appreciate the explicit reference in the Agency's Initial Statement of Reasons to global privacy controls as an example of an opt-out preference signal. However, we think this section, or 7025(b), requires more clarification and confirmation that a "do not track" signal is not sufficient to be considered a request to opt-out of data selling and sharing.



## ***Article 2: Required Disclosures to Consumers***

### **7011 Privacy Policy**

(e)(1)(H), (I), and (J): For the purposes of the privacy policy, we believe that these three paragraphs which reference disclosure of personal information are overly broad, and these types of disclosures should be limited to sale and share, as indicated in (D), (E), and (F). We believe this is more in keeping with the underlying purpose of the CCPA and CPRA and provides consumers with more specific and useful information. We also believe that these disclosures could inadvertently create significant cybersecurity risks.

(e)(3)(F) and (G): We believe businesses that do not sell or share personal information should be clearly exempted from these requirements to disclose in their privacy policy how the business would process opt-out preference signals. As drafted this requirement would create significant confusion for consumers about whether their Personal Information is being sold or shared.

### **7012 Notice at Collection of Personal Information**

In instances where the only in-scope personal information that a business is collecting is for the purpose of cross context behavioral advertising, we believe that companies should not be required to post a notice at collection since this is already required in the privacy policy as well as the opt-out notice which provide the same information. Adding yet another notice in this case simply adds confusion for the consumer and is an unnecessary burden on companies.

### **7013 Notice of Right to Opt-Out of Sale/Sharing and the Do Not Sell or Share My Personal Information Link**

For businesses that may find compliance with icon size requirements in 7015 challenging, but only share data, it would be confusing to consumers if these businesses were required to use the language that indicates to consumers that they are engaged in the sale of data. We request that 7013 allow businesses to post a link stating only, "Do Not Share My Personal Information" if the business is not engaged in the sale of data.

## ***Article 3: Business Practices for Handling Consumer Requests***

### **7021 Timeline for Responding to Requests**

(b) We are concerned that validation of requests due to missed calls or lack of response to emails may take a significant amount of time. While we appreciate the provision allowing up to 90 days, it's conditioned upon the business providing a consumer an individual notice and explanation of the reason an additional 45 days is required. This is overly burdensome especially in instances where the delay is no fault of the business. We request the 45-day timeline start after validation is complete, while still permitting an additional 45-day extension if the business provides the appropriate notice and explanation.

### **7022 Right to Delete**

(d) The language allowing a business to delay compliance with a request to delete if data is stored on an archive or backup is welcome, however the requirement that the business apply a request to delete when an archived or backup system becomes active, is too administratively burdensome. A company could for example find itself out of compliance when data is restored years after the fact for a non-business purpose like internal audits or responding to litigation. We request that this standard become a two-part test in line with the current language. The personal information must be restored to an active system **and** next accessed or used for a sale, disclosure, or commercial purpose.

### **7023 Requests to Correct**

(c)(2) As above, we believe that even with these latest changes to more closely mirror 7022 (d) businesses should only have to respond to requests to correct when personal information is restored to an active system **and** next accessed or used for a sale, disclosure, or commercial purposes.

### **7024 Requests to Know**

(i) We believe that the language detailing what a service provider or contractor must provide a business in responding to a request to know is overly prescriptive. We propose that the last clause of the sentence be stricken and the paragraph just state that the service provider or contractor must provide assistance.

### **7025 Opt-out Preference Signals**

(e) As stated in our previous letter, we believe the language in this section and the agency's ISOR misreads and misinterprets the mechanics of Civil Code section 1798.135(b). This section clearly says businesses have the option to choose (a) links to opt-out or (b) recognition of preference signals. The ISOR contains a caveat to the agency's argument that signal reading is mandatory by tying it to frictionless or non-frictionless preference signals. However, 1798.135 never references or contains the words "frictionless" or "non-frictionless". Friction is a concept generated in the draft regulations and it is unclear why this concept of friction status should override the statute's plain language in Civil Code section 1798.135(b).

The ISOR also attempts to bolster the argument that businesses do not have an option to comply with 1798.135 (a) or (b) by blending 1798.135 (e) into the reasoning, but (e) is about honoring link usage or preference signals effectuated on another's behalf. And then still, (e) doubles down and says "[f]or purposes of clarity" that a business can elect to follow 1798.135 (a), and in (e), there is no tie back to (b). To give meaning to the statute as written, we urge the Agency to preserve the option of posting the above-referenced links in lieu of processing preference signals.

### **7026 Requests to Opt-Out of Sale/Sharing**

(f) This provision requires businesses to notify all third parties to whom the business has shared a consumer's personal information after the consumer opts out of sale/sharing. We are concerned that this provision does not make sense in the context of cross-context behavioral advertising where the opt-out will be almost instantaneous and occur on a technological level. For example, cross-context advertising cookies/pixels will stop being deployed to the user when they opt-out, and the sharing with third parties will stop. In this context we think the requirement to have to inform third parties about the opt-out does not make sense and it should be sufficient to actually opt out the consumer from cross-context behavioral advertising on the business's website, and stop sharing the consumer's personal information with third parties for cross-context behavioral advertising purposes. The goal appears to be to stop showing the consumer ads based on their activities across websites, and therefore there is no added benefit to having to formally notify third parties in this context.

### **7027 Requests to Limit Use and Disclosure of Sensitive Personal Information**

(a) We ask that the agency define a "heightened risk of harm" to consumers as it relates to the use or disclosure of sensitive personal information.

### ***Article 5 Verification of Requests***

#### **7063 Authorized Agents**

Although we appreciate the discussion by the Board on October 29<sup>th</sup> regarding new protections the agency has added for sensitive information in requests to correct 7023 (j) that mirror the protections for requests to know in 7024 (d), we continue to be very concerned that in the context of financial institutions this section still leaves open a backdoor for bad actors to access consumers' sensitive personal information. We believe that this class of

business should be permitted to take a risk-based approach to processing authorized agent requests to minimize the risk of unintentional release of consumers' sensitive personal information.

(b) As noted in our previous letter this paragraph does not provide a clear mechanism for businesses, but of particular importance, financial institutions, to verify that a consumer has provided the authorized agent with a power of attorney. We have very strong concerns that this language could result in unauthorized disclosure of financial information. Therefore, we request clarification that the authorized agent in the context of subsection (b) must provide evidence of a power of attorney pursuant to Probate Code sections 4121 to 4130.

**Article 8: Training and Record Keeping**

**7102 Requirements for Businesses Collecting Large Amounts of Personal Information**

(a) We are requesting clarification on the number of consumers that trigger reporting requirements. Is the reference to 10 million consumers a reference to Californian consumers, consumers in the United States or consumers globally?

**Article 9: Training and Record Keeping**

**7301 Investigations**

(b) As noted above we continue to have very strong concerns with the reduced compliance window these late regulations are pushing on businesses. Although we welcomed the board's discussion on October 29<sup>th</sup> about the lack of time businesses will be given for compliance, we believe this section does not go far enough. From our reading of 1798.185 (d) we believe there is nothing in this language that precludes the agency from further delaying enforcement. The language says that an action "shall not commence until July 1, 2023" but it does not say the agency "must commence" enforcement on or after July 1, 2023. In contrast, in the same section, the Agency is required to adopt regulations by July 1, 2022. That date is explicit and immutable. It seems fundamentally unfair that the Agency can miss a clear statutory deadline yet not provide clear assurances to the business community that they will not begin enforcement until 1 year after regulations are adopted when no language in the statute precludes this.

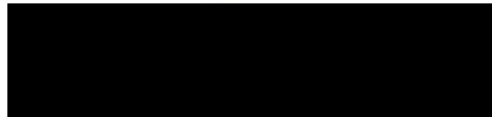
**Conclusion**

As noted above we appreciate the work of the agency board and staff to integrate many of the suggestions raised in our previous letter into this new revised text. While there has been improvement, we urge the agency to not rush forward with this current draft but instead continue to work methodically and holistically until the regulations are more complete. Coupling this with a delay in enforcement is the best way to stand up this new regulatory regime, while protecting consumers and giving businesses the necessary and required timeline for compliance. Thank you, in advance, for your consideration of our comments. We would be happy to answer any questions.

Sincerely,



John W. Mangan  
Regional Vice President, State Relations  
American Council of Life Insurers



Matthew R. Powers  
Vice President  
Association of California Life and Health Insurance  
Companies

---

**From:** Avonne Bell <[REDACTED]>  
**Sent:** Monday, November 21, 2022 6:06 AM  
**To:** Regulations  
**Subject:** Modification to Proposed Regulations Implementing CPRA  
**Attachments:** FINAL CTIA 112323 Comment on Modified CPRA Regulations.pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender [REDACTED]

Good morning,

Attached are CTIA's comments in response to the Notice of Modification to the Proposed Regulations implementing the Consumer Privacy Rights Act of 2020. Please let us know if you have questions.

Thank you,  
Avonne Bell



**Avonne Bell**

Director, Connected Life

1400 16<sup>th</sup> Street, NW

Washington, DC 20036

[REDACTED] (office)

[REDACTED] (mobile)

Before the  
**California Privacy Protection Agency**

In the Matter of

California Privacy Rights Act of 2020  
Rulemaking Process

)  
)  
)  
)  
)  
)

Invitation for Comments on  
Proposed Rulemaking

**COMMENTS OF CTIA to  
MODIFIED REGULATIONS ISSUED OCTOBER 29, 2022**

Gerard Keegan  
Vice President, State Legislative Affairs

Avonne Bell  
Director, Connected Life

Jake Lestock  
Director, State Legislative Affairs

**CTIA**  
1400 16th St. NW, Suite 600  
Washington, DC 20036  
(202) 736-3200  
[www.ctia.org](http://www.ctia.org)

November 21, 2022

## TABLE OF CONTENTS

|  | <u>Page</u> |
|--|-------------|
| INTRODUCTION.....  | 4           |
| I. CTIA Concerns Relating to the Modified Regulations.....   | 5           |
| A. § 7002: The “Reasonable Consumer Expectations” Test .....   | 5           |
| 1. Notices to Consumers are the Proper Tool for Setting Permissible<br>Data Uses, while a Multi-Factor Consumer Expectations Test<br>Should be Part of a Post-Collection Compatibility Framework .....       | 6           |
| 2. Unless Notices to Consumers are Determinative for Setting<br>Consumer Expectations, the Agency’s Consumer-Expectations<br>Test Creates Undue Regulatory Ambiguity and Risks Arbitrary<br>Enforcement..... | 8           |
| 3. The Use of Service Providers is Not Relevant to Consumers’<br>Reasonable Expectations .....   | 10          |
| B. § 7004: Privacy Policies and Requests to Know .....   | 11          |
| 1. As Modified, Section 7004 Improperly Imposes “Consent”<br>Requirements across “Choice Architecture” .....   | 11          |
| 2. When Evaluating Consumer Choice Architecture, Reasonable<br>Efforts to Offer Meaningful Choices to Consumers Should be<br>Recognized.....   | 13          |
| 3. Proactively Establishing Processes to Review User Interfaces<br>Should be Viewed as Privacy-Protective, and Weighed Favorably<br>by the Agency .....  | 13          |
| 4. On/Off Toggles Should Not be Called into Question as Potential<br>Dark Patterns.....  | 14          |
| 5. Scrolling When Submitting Opt-Outs Should Not be Considered a<br>Dark Pattern .....   | 15          |
| C. §§ 7022-7024: Consumer Requests .....   | 15          |
| D. §§ 7022, 7026: Flow-Down Requirements to Service Providers and Third<br>Parties in Rights Request Fulfillment .....   | 16          |
| E. § 7051: Imputed Responsibility for Service Providers and Contractors.....   | 16          |
| F. § 7025: Opt-Out Preference Signals .....  | 17          |
| II. The Modified Regulations Do Not Address Important Issues from the Draft<br>Regulations .....   | 18          |

A. § 7025: Opt-Out Preference Signals ..... 18

B. §§ 7011, 7024: Privacy Policies and Requests to Know ..... 19

C. § 7023: Right to Correct ..... 20

D. § 7027: Permitted Sensitive Personal Information Uses..... 20

CONCLUSION.....21

Before the  
**California Privacy Protection Agency**

|   |   |   |
|---|---|---|
| In the Matter of  | ) |   |
|   | ) |   |
| California Privacy Rights Act of 2020<br>Rulemaking Process | ) | Invitation for Comments on<br>Proposed Rulemaking |
|   | ) |   |
|   | ) |   |
|   | ) |   |

**INTRODUCTION**

CTIA<sup>1</sup> appreciates the opportunity to provide these comments on the California Privacy Protection Agency’s (the “Agency’s”) modified text of the draft regulations to implement the California Privacy Rights Act (CPRA) issued October 29, 2022 (the “Modified Regulations”). The Modified Regulations implement changes the Agency made to the draft regulations it issued on July 8, 2022 (the “Draft Regulations”).

CTIA previously submitted comments regarding the Draft Regulations on August 23, 2022 (“Prior Comment”), and CTIA appreciates the Agency’s efforts to address a number of issues raised in its Prior Comment. This comment primarily addresses issues arising from changes between the Draft and Modified Regulations. CTIA also briefly outlines some important issues it addressed in its Prior Comment that remain unaddressed by the Modified Regulations.

---

<sup>1</sup> CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st-century connected life. The association’s members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry’s voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry’s leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.



## **I. CTIA Concerns Relating to the Modified Regulations**

CTIA has identified some issues related to provisions that the Agency included in the Modified Regulations as well as some that remain unchanged from the Draft Regulations. CTIA thus provides comments pertaining to the following sections of the Modified Regulations, addressed in detail in the following order below:

- § 7002: Restrictions on the Collection and Use of Personal Information;
- § 7004: Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent;
- §§ 7022: Requests to Delete;
- § 7023: Requests to Correct;
- § 7024: Requests to Know
- § 7051: Service Providers and Contractors;
- § 7026: Requests to Opt-Out of Sale/Sharing;
- § 7025: Opt-Out Preference Signals.

### **A. § 7002: The “Reasonable Consumer Expectations” Test**

CTIA appreciates the Agency’s removal of an “average consumer expectations” standard for data uses, which CTIA argued in its Prior Comment materially departed from CPRA’s structure as a notice-based statute. Unfortunately, Section 7002(b) of the Modified Regulations appears to have substituted a multi-factor “reasonable” consumer expectations test for the “average” consumer expectations test that was previously in the Draft Regulations.

CTIA agrees with the Agency that consumer expectations should be relevant in how organizations use data. However, CTIA submits that a multi-factor consumer-expectations test as contained in the Modified Regulations is more properly part of a compatibility framework

governing new uses of previously-collected data – not a general standard to be applied across all data uses whatsoever. Instead, the notices presented to consumers at collection meaningfully shape consumers’ expectations about how the organization collecting their data will use it. Notices should thus continue to generally determine how organizations can use the data they collect from consumers, while the Modified Regulations’ multi-factor consumer expectations test should apply to post-collection governance of new data uses.

This is the approach taken by Europe’s General Data Protection Regulation (GDPR), as well as more recently by Colorado’s draft privacy regulations. Placing a multifaceted consumer-expectations analysis within this type of post-collection compatibility framework would thus align the Agency’s rulemaking with other, globally-recognized privacy regimes, and prevent companies from facing potentially conflicting standards governing their data practices. Unless notices to consumers retain their role as the anchor for generally determining permissible data uses, the Modified Regulations will create unacceptable regulatory ambiguity for companies making good-faith efforts to comply with CPRA. And, in any case, the use of service providers should not be considered as impacting consumers’ reasonable expectations.

**1. Notices to Consumers are the Proper Tool for Setting Permissible Data Uses, while a Multi-Factor Consumer Expectations Test Should be Part of a Post-Collection Compatibility Framework**

CTIA respectfully submits that the notices presented to consumers at collection adequately and meaningfully set consumers’ general expectations at the point of collection about how businesses will use their data. Indeed, the Modified Regulations state that notices-at-collection “provide consumers with timely notice ... about ... the purposes for which the personal information is ... used,” and give consumers “a tool to exercise meaningful control over the

business’s use of their personal information.” § 7012(a). This implicitly acknowledges the impact notices have on consumer expectations; the “meaningful control” notices offer comes from the fact that notices let consumers know what to expect from a company, and from those notices, consumers can make decisions about whether they want to interact with the company. Thus, notices to consumers should be considered as anchoring how consumers reasonably expect businesses to use their information, and should thus continue to set permissible data uses.

In contrast, a multi-factor consumer-expectations test is more properly employed as part of a post-collection compatibility framework that assesses whether new uses of previously-collected data are proper. This point can be most clearly demonstrated by looking at how two other privacy regimes, the EU GDPR and Colorado’s draft privacy regulations, place a multi-factor test involving consumer expectations squarely within a post-collection compatibility analysis for new data uses:

- **GDPR.** GDPR requires businesses to present notices to consumers “at the time when personal data are obtained.” *See* Art. 13(1) GDPR. These notices generally determine the purposes for which personal data may be processed. However, when previously-collected personal information is processed for a new “purpose other than that for which the personal data [were originally] collected,” the GDPR applies a multi-factor compatibility test. *See* Art. 6(4) GDPR. One factor businesses must consider when assessing compatibility is “the reasonable expectations of [consumers] based on their relationship with the [business]” as to the “further use” of personal information in the post-collection context. *See* Recital 50 GDPR.
- **Colorado.** Similarly, the draft Colorado privacy regulations require notices to be presented to consumers “before the time the Personal Data is collected from Consumers.” 4 CCR 904/3, Rule 6.08(A). These notices must specify processing purposes, *see id.*, and the purpose

descriptions within notices thus generally determine how personal information can be used. However, when previously-collected data is to be used for a “new Processing purpose,” the draft Colorado regulations apply a multi-factor test to assess whether the new use is “necessary to or compatible with the original specified purpose.” *Id.* Rule 6.08(C). One factor businesses must consider when assessing compatibility is “[t]he reasonable expectation of an average Consumer concerning how their Personal Data would be used once it was collected.” *Id.*

Lastly, using a multi-factor consumer-expectations test as a governance tool for post-collection new uses of data is a better fit with CPRA’s rulemaking grant. CPRA suggests that consumer-expectations rulemaking should focus on new “business purposes ... for which businesses ... may use consumers’ personal information,” or on “*other* notified purposes” beyond the purposes described a collection. *See* Civ. Code § 1798.185(a)(10).

CTIA therefore respectfully submits that the Agency should consider placing the Modified Regulations’ multifactor consumer-expectations test within the context of a post-collection compatibility framework. This would align the Modified Regulations with other global privacy regimes and CPRA’s rulemaking grant, while encouraging businesses to clearly communicate their intended data uses to consumers.

## **2. Unless Notices to Consumers are Determinative for Setting Consumer Expectations, the Agency’s Consumer-Expectations Test Creates Undue Regulatory Ambiguity and Risks Arbitrary Enforcement**

Applying Section 7002(b)’s consumer-expectations test generally to all data uses would create regulatory ambiguity for companies and consumers that makes compliance with CPRA difficult to achieve, particularly for small- and medium-sized businesses, and for companies making good-faith efforts to build proactive compliance.

Applying a consumer-expectations test generally across data uses, even when clear notice has been given to consumers at collection, gives the Agency inordinate discretion to ignore privacy disclosures to consumers, and to substitute its own judgement about the reasonable expectations of a consumer. Companies attempting to comply with CPRA will find themselves guessing not about *what consumers actually expect*, but rather *what the Agency thinks consumers may expect* from them. Since the Modified Regulations do not permit companies to presume that clear disclosures to consumers will set consumers' reasonable expectations, nor do they require the Agency to engage in empirical research prior to making findings about consumers' purported reasonable expectations, entities lack an objective basis by which they can reliably anticipate what the Agency will expect of them in terms of compliance. To the extent that a consumer-expectations test is retained in the Modified Regulations, CTIA recommends that the notices and disclosures to consumers that CPRA already plentifully requires should be the determining factor for consumers' expectations.

The Agency's modifications to Section 7002 further compound ambiguity by introducing a multi-factor test for determining what consumers' expectations might be. The test includes factors such as: (1) the relationship between the consumer and the business; (2) the type and nature of personal information that the business seeks to collect or process; (3) the source of the personal information and the method of collection or processing; (4) the specificity, explicitness, prominence, and clarity of disclosures to the consumer(s) about the purpose for collecting or processing their personal information; and (5) the degree to which the involvement of service providers, contractors, or third parties in collecting or processing personal information is apparent to the consumer. § 7002(b). This approach requires an extensive analysis by companies even for primary collection purposes, and fails to give appropriate weight to the one factor the Modified

Regulations itself mandates to give consumers “meaningful control over the business’s use of their personal information”—that is, the notice presented at collection. *See* § 7012(a). In practice, this modification to Section 7002 seems intended to move CPRA from the statutory notice standard that it is, to a regime requiring more opt-ins than the statute ever contemplated.

It is perhaps for these reasons that, as discussed above, other globally-recognized privacy regimes like the GDPR place a consumer expectations analysis within a post-collection compatibility framework specifically for new uses of previously-collected data. The Regulations should align with these approaches and adopt a compatibility test that considers consumer expectations when new uses of previously-collected data are envisaged, rather than applying a multi-factor consumer-expectations test across all data uses.

### **3. The Use of Service Providers is Not Relevant to Consumers’ Reasonable Expectations**

If the Agency decides to move forward with the reasonable consumer expectations standard under the multi-factor test, Section 7002(b)’s list of expectations-driving factors should not include whether service providers or contractors are involved in collecting or processing consumers’ personal information. A business’s reliance on service providers, under appropriately protective contracts, does not factor into a consumer's reasonable expectation regarding data uses. For example, it is likely irrelevant to consumers whether an ecommerce company operates its own warehouse or has contracted warehousing operations out to a service provider – instead, consumers simply want to receive their orders on time. This factor would particularly damage small and medium sized businesses, which often must rely on service providers for many of their core business processes.

**B. § 7004: Privacy Policies and Requests to Know**

CTIA agrees with the Agency that it is important to provide consumers with meaningful opportunities to exercise the privacy rights offered to them by CPRA. CTIA is concerned, however, that the modified Section 7004 alters the balance between consent and choice that CPRA establishes, and fails to recognize companies' efforts to design effective choice architecture for consumers. As described in more detail below, CTIA is first concerned that the modified Section 7004 conflates "choice" with "consent" in its provisions relating to choice architecture. This should be changed so as not to unduly limit consumers' choices, and to not require more opt-ins than CPRA mandates. Second, CTIA submits that the Modified Regulations should recognize proactive efforts by businesses to make their choice architecture meaningful and effective for consumers, such as when businesses employ reasonable efforts to comply with Section 7004, or when businesses establish internal processes to review their user interfaces. Lastly, CTIA submits that common features of rights submission interfaces, like toggles and webpage disclosures that can result in modest scrolling, should not be seen as practices interfering with consumer choice.

**1. As Modified, Section 7004 Improperly Imposes "Consent" Requirements across "Choice Architecture"**

CTIA is concerned that the Agency's modified approach to Section 7004 conflates "choice architecture" with "consent" – and thus, improperly treats all consumer "choices" as if they must meet the heightened requirements for the very limited situations where CPRA requires "consent." *See* Cal. Civ. Code § 1798.121(b); § 1798.135(c). CPRA does not mandate that all choices a consumer can make relating to personal information involve a full "consent." For example, opt-outs do not require a specific consent from a consumer; instead, the consumer can generally choose to tell a business to stop all sales of personal information.

However, the Modified Regulations suggest that consumer choice architecture needs to be benchmarked to CPRA-mandated consent requirements—for example, all consumer choice options would need to be “specific” and “informed,” among other requirements. This can be seen in the proposed language to Section 7004(a)(4), which suggests that if a choice offered to a consumer does not meet full consent standards (“freely given, specific, informed, and unambiguous”), the choice could be considered “impair[ed]”:

*Businesses should also not design their [choice architecture] methods in a manner that would impair the consumer’s ability to exercise their choice because consent must be freely given, specific, informed, and unambiguous.*

While CTIA agrees that interfaces should not seek to impair or interfere with meaningful consumer choice, CTIA submits that the Agency’s approach to consumer choice in 7004(a)(4) remains improper for two reasons. First, this approach could adversely impact consumer choices. For example, would all choices offered to consumers now need to be “specific?” If so, would businesses need to start requiring consumers to make “specific” opt-outs to specific data sales? Second, this approach could be interpreted as a backdoor and extra-statutory requirement for additional opt-in consents throughout consent architecture. CTIA therefore recommends that Section 7004(a)(4) be updated as follows:

*Avoid choice architecture that impairs or interferes with the consumer’s ability to make a choice. Businesses should also not design their methods in a manner that would impair the consumer’s ability to ~~exercise their choice because~~ **consent freely given, specific, informed, and unambiguous** where required by the CCPA.*

CTIA further notes that the conflation of “choice” and “consent” is not restricted to Section 7004(a)(4), but is present throughout Section 7004. Therefore, CTIA requests that the Agency apply consent requirements only to situations where CPRA mandates consent, while permitting other consumer choices, like opt-outs, to be made under the conditions permitted by the CPRA.



**2. When Evaluating Consumer Choice Architecture, Reasonable Efforts to Offer Meaningful Choices to Consumers Should be Recognized**

CTIA submits that businesses' reasonable efforts to offer meaningful and effective choices to consumers should be recognized, particularly in an area as context-specific as consumer choice architecture. Failing to consider a business' good faith efforts to offer meaningful choice risks arbitrary enforcement, particularly since businesses of different scope and scale will necessarily require different mechanisms interfacing with consumers. CTIA suggests that the Agency should tie the requirements of Section 7004 to a "reasonable efforts" standard, and the Agency should consider businesses' good faith compliance efforts. CTIA recommends the following revision to Section 7004(a):

*Except as expressly allowed by the CCPA and these regulations, businesses shall **make reasonable efforts** to design and implement methods for submitting CCPA requests and obtaining consumer consent that incorporate the following principles.*

**3. Proactively Establishing Processes to Review User Interfaces Should be Viewed as Privacy-Protective, and Weighed Favorably by the Agency**

In addition to making reasonable efforts to comply, if businesses proactively build processes to review their user interfaces, this should be seen as a positive and privacy-protective practice and should be weighted in businesses' favor when the Agency makes determinations as to whether a user interface constitutes a dark pattern. Including this as a factor for consideration encourages businesses to actively review for dark patterns and make informed choices about the interfaces they deploy. Expressly recognizing review processes as relevant provides an ongoing incentive for businesses to protect consumers from developments that occur after the initial launch of an interface, which should be encouraged by the Agency. Therefore, CTIA suggests modifying Section 7004(c) as follows:

*A user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decision making, or choice. A business's intent in designing the interface is not determinative in whether the user interface is a dark pattern, but a factor to be considered. **If a business can show that it had a process for reviewing user interfaces for dark patterns, this may weigh against establishing the existence of a dark pattern.** If a business did not intend to design the user interface to subvert or impair user choice, but the business knows of and does not remedy a user interface that has that effect, the user interface may still be a dark pattern. Similarly, a business's deliberate ignorance of the effect of its user interface may also weigh in favor of establishing a dark pattern.*

#### **4. On/Off Toggles Should Not be Called into Question as Potential Dark Patterns**

Section 7004(a)(3) of the Modified Regulations suggest that on/off toggles “may be confusing to a consumer,” and could, thus, be evaluated as a dark pattern. While CTIA shares the Agency’s goal of maintaining clear and meaningful choice for consumers, CTIA respectfully submits that Section 7004(a)(3)’s focus on toggles is overly restrictive. On/off toggles are a privacy mechanism, and are intended to clearly give consumers a simple method for exercising choice. Consumers regularly interact with toggles through their online activities. Indeed, other provisions of the Modified Regulations expressly permit companies to use “a toggle or radio button” to let consumers know their opt-out preferences have been executed. *See* §§ 7025(c)(6), 7026(g), 7027(h).

CTIA notes the Modified Regulations already require that “[t]oggles or buttons must clearly indicate the consumer’s choice.” § 7004(a)(3)(B). This language is sufficient to protect against confusing practices. Accordingly, CTIA requests that the Agency reconsider calling on/off toggles into question as potentially confusing to consumers.

## 5. Scrolling When Submitting Opt-Outs Should Not be Considered a Dark Pattern

Section 7004(a)(5) of the Modified Regulations states that companies potentially “undermine the consumer’s choice” if – after a consumer clicks on a “Do Not Sell” link – the consumer must “search or scroll through the text of a ... webpage” to locate the mechanism to submit an opt-out. CTIA submits that prohibiting *any* scrolling in connection with exercising opt-out rights is overly prescriptive. Some reasonable degree of scrolling may be necessary to accommodate other requirements of CPRA or the Modified Regulations, including clearly describing rights or potential impacts of exercising rights. Also, screen size and device differences will make scrolling vary from one user experience to another. CTIA thus suggests that Section 7004(a)(5)(A) be updated as follows:

*Upon clicking the “Do Not Sell or Share My Personal Information” link, the business shall not require the consumer to **unreasonably** search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out of sale/sharing.*

### C. §§ 7022-7024: Consumer Requests

The Modified Regulations continue to saddle businesses with onerous and unworkable obligations related to Requests to Know, Delete, and Correct. While CTIA agrees that businesses should generally be required to make reasonable efforts to notify service providers and third parties of a consumer’s request to delete personal information, the Modified Regulations would require businesses to offer detailed explanations about why certain consumer requests cannot be fulfilled.

Among other things, a business must provide a consumer with detailed explanations as to:

- a) why it cannot notify all third parties of a Deletion request (§ 7022(b), (c));
- b) why it cannot delete all personal information (particularly when a legal exception applies) (§ 7022(f)(1));

- c) why it cannot provide personal information beyond a 12-month lookback period (§ 7024(h)); and
- d) when denying correction requests, why the data is not being corrected (§ 7023(f)).

The onus of these requirements is not commensurate to any consumer benefit.

**D. §§ 7022, 7026: Flow-Down Requirements to Service Providers and Third Parties in Rights Request Fulfillment**

CTIA is concerned that exemptions to “flow-down” requirements in the context of consumers’ rights requests are inconsistent and not evenhandedly applied across all CPRA-mandated rights. The Modified Regulations generally require verifiable consumer requests (Know, Delete, Correct) to be flowed-down to service providers and contractors for fulfillment. *See* §§ 7022, 7023, 7024. Further, the Modified Regulations require non-verifiable request types (Opt-Out, Request to Limit), as well as one verifiable request type (Delete), to be flowed-down to third parties. *See* §§ 7022, 7025, 7027.

Despite these overarching flow-down requirements, the Agency recognizes that there should be exceptions to these requirements, as the Modified Regulations introduce a new “disproportionate effort” carve-out, but only for deletion requests.

*If a business claims that notifying some or all third parties would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot notify all third parties.*

*See* § 7022(b)(3).

CTIA submits that the concerns motivating this carve-out are equally applicable across all request types – not just Deletion. The Agency should, therefore, extend the carveout to the other verifiable and non-verifiable requests available under CPRA.

**E. § 7051: Imputed Responsibility for Service Providers and Contractors**

Section 7051(c) addresses scenarios where businesses may be considered to have reason to know their service providers were in violation of CPRA. These scenarios fail to consider that businesses may have conducted due diligence as part of selecting or onboarding their service provider, and to recognize such due diligence as a factor weighing against knowledge that a service provider may be in violation of CPRA. Instead, Section 7051(c) only considers contract enforcement and audits relevant in attributing liability to businesses.

This approach seems incomplete. Due diligence is often conducted prior to engaging a third-party vendor, and in some industries is a requirement. The Agency should consider this common practice when assessing whether a business has reason to know a service provider is in violation of CPRA, and as such Section 7051(c) should be updated to include a reference to vendor due diligence, as follows:

*Whether a business conducts due diligence of its service providers and contractors factors into whether the business has reason to believe that a service provider or contractor is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract, **nor performed service provider and contractor due diligence before engagement**, nor exercises its rights to audit or test the service provider's or contractor's systems might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the service provider or contractor.*

#### **F. § 7025: Opt-Out Preference Signals**

The Regulations appear to presume that consumers are “known to” businesses simply because the consumer has logged into an account. This is not a proper presumption. Just because a consumer can log into an account does not mean the consumer is “known to” the business. The example of Section 7025(c)(7)(C) should thus be updated as follows:

*Angela also has an account with Business O and has enabled an opt-out preference signal on her browser while logged into her account. Business O applies the opt-out preference signal as a valid request to opt-out of sale/sharing not only to Angela's current browser, but also to Angela's account because she is ~~known to the business~~ **logged in** while making the request. Angela later logs into her account with Business O using a different device that does not have the opt-out preference signal enabled. Business O shall not interpret the absence of the opt-out preference signal as consent to opt-in to the sale of personal information.*

## **II. The Modified Regulations Do Not Address Important Issues from the Draft Regulations**

CTIA notes that a number of important issues raised in CTIA's Prior Comment remain unaddressed. For these issues, CTIA's concern is that the Agency is exceeding its authority, enacting rules inconsistent with CPRA's statutory text, or failing to fulfill CPRA's express rulemaking mandates. CTIA, therefore, renews its previous concerns regarding the following sections of the Modified Regulations:

### **A. § 7025: Opt-Out Preference Signals**

CTIA's Prior Comment at sec. I.D.2. discussed how the draft regulations did not fulfill CPRA's rulemaking mandates for opt-out preference signals. The Modified Regulations' provisions for opt-out preference signals continue to leave unfulfilled, and at times actively conflict with, CPRA's statutory requirements for opt-out preference signal technologies:

- CPRA contains detailed statutory specifications for opt-out preference signals that remain unaddressed in the Modified Regulations. The Modified Regulations continue to fail to address CPRA requirements to ensure that opt-out preference signal technology (1) "cannot unfairly disadvantage another business;" (2) is "free from defaults;" and (3) "does not require that the consumer provide additional information beyond what is necessary." Civ. Code § 1798.185(19)(A)(i)-(iii). The Modified Regulations do not contain anything that resembles a "technical specification" for opt-out preference signals. Civ. Code § 1798.185(19)(A). At

times, the Regulations appear to contradict CPRA’s statutory text. For example, CPRA prohibits opt-out preference technology from turning the opt-out preference signal “on” by default. Civ. Code § 1798.185(19)(A)(iii). But, the Regulations leave open the possibility that preference signal technology could do just that. The Regulations could let opt-out preference signals be “on” by default, as long as the opt-out technology “make[s] 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 Modified Regulations failed to add technical requirements that enable businesses to know when opt-out signals are being sent from Californians. At present, the Regulations offer no specifications that allow the current recognized formats for preference signals – HTTP headers and javascript objects – to also transmit a requestor’s residency. This could be easily changed by adding a customer/structured field in the HTTP header.

#### **B. §§ 7011, 7024: Privacy Policies and Requests to Know**

As discussed in sec. I.C. of CTIA’s Prior Comment, Section 7011 of the Modified Regulations continues to require inconsistent levels of detail in privacy policies. Section 7011(e)(1)(E)& (I) require privacy policies to identify categories of personal information they collect, and then – for “each category” – list the categories of third parties that may receive that personal information. Similarly, and in addition to the issues raised in its Prior Comment, when responding to Requests to Know, Section 7024(k)(5), (6) require businesses to identify categories of personal information they hold, and then – for “each category” – list the categories of third parties that may receive that personal information. Requiring this level of granularity for information disclosures is inconsistent with other disclosures that must be made to consumers.

**C. § 7023: Right to Correct**

As discussed in CTIA’s Prior Comment at sec. III.B., Section 7023(h) of the Modified Regulations continues to require businesses to tell persons who they think are making “fraudulent” requests “why it believes the request is fraudulent.” This could dangerously subvert businesses’ security and fraud prevention. Similarly, Section 7023(j) continues to permit consumers to make follow-on Right to Know requests to test whether Correction requests have been processed. This enables repetitive requests and upsets the balance set by CPRA limiting the number of Right to Know requests permitted per year.

**D. § 7027: Permitted Sensitive Personal Information Uses**

As discussed in sec. III.C. of CTIA’s Prior Comment, security-related uses of sensitive personal information that are unaffected by a Request to Limit continue to be unduly narrowed by the Modified Regulations. CPRA permits sensitive personal information to be used to “[h]elp[] ensure security and integrity” independent of a Right to Limit. Civ. Code §§ 1798.121(a), 1798.140(e)(2). However, the Regulations in Section 7027(m)(2) permit businesses to use sensitive personal information “[t]o prevent, detect, and investigate security incidents” without triggering a Right to Limit. Section 7027(m)(2) should be made consistent with CPRA’s statutory text.



**CONCLUSION**

CTIA appreciates the Agency's consideration of these comments and stands ready to provide any additional information that would be helpful.

Respectfully submitted,

/s/ Gerard Keegan

Gerard Keegan  
Vice President, State Legislative Affairs

Avonne Bell  
Director, Connected Life

Jake Lestock  
Director, State Legislative Affairs

**CTIA**  
1400 16th St. NW, Suite 600  
Washington, DC 20036



November 21, 2022

---

**From:** Irene Ly <[REDACTED]>  
**Sent:** Monday, November 21, 2022 6:37 AM  
**To:** Regulations  
**Cc:** Jolina Cuaresma  
**Subject:** CPPA Public Comment - Common Sense Media  
**Attachments:** CPPA Comments - Common Sense Media.pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear Mr. Soublet,

Please see the attached for Common Sense Media's written comments on the Agency's modified proposed regulations. Thank you for the Agency's time and consideration of these comments.

Best,

**Irene Ly**

Policy Counsel | Common Sense Media



November 21, 2022

California Privacy Protection Agency  
c/o Brian Soublet  
2401 Arena Blvd  
Sacramento, CA 95834  
via email at regulations@coppa.ca.gov

Dear Mr. Soublet:

Common Sense Media submits these comments on the California Privacy Protection Agency's (Agency) modified proposed regulations that, if finalized, would implement the California Privacy Rights Act (CPRA), which strengthened the California Consumer Protection Act (CCPA). We are the nation's leading independent nonprofit organization dedicated to helping kids and families thrive in an increasingly digital world. We empower parents, teachers, and policymakers by providing unbiased information, trusted advice, and innovative tools to help them ensure that media and technology are positive forces in children's lives.

On August 23, 2022, Common Sense Media submitted comments (August Comments) in response to the Agency's July 8, 2022 Proposed Regulations. On October 21, 2022, the Agency issued Modified Proposed Regulations, which included a correct citation for "COPPA" and a retitled section 7071 to make clear that it protects teens until the day that they turn 16 years old. While we are pleased to see two of our recommendations followed, we are concerned that the Agency disagreed with our more substantive recommendations. We applaud the Agency's efforts to solicit comments on its Modified Regulations and we appreciate the opportunity to provide additional detail on our August Comments.

**Comments to §§ 7070 and 7071.**

***We recommend the Agency define the term "actual knowledge" to include the meaning of "willfully disregard."*** Section 1798.120(c) of the CCPA, as amended by the CPRA, mandates certain requirements when a business has "actual knowledge" that a consumer is under 16 years of age. It also provides that "[a] business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age." This makes California's privacy law stronger than the federal Children's Online Privacy Protection Act (COPPA), which does not include "wilful

disregard,” language, allowing a firm to bury its head in the sand and claim it did not know kids were on its platform while touting to advertisers about its kids audience.<sup>1</sup>

Sections 7070 and 7071 of the Modified Proposed Regulations do not include any reference to the “willfully disregard” language. The Agency’s regulations should make clear that if a business purposefully, deliberately, or intentionally disregards a consumer’s age, it would be deemed to have actual knowledge. To make the regulations consistent with CCPA, as amended by the CPRA, we offer the following definition for consideration:

“‘Actual knowledge’ means actual awareness, understanding, or recognition of a fact. The term also includes willful, purposeful, deliberate, or intentional disregard of a fact.”

Defining “actual knowledge” to include conduct that amounts to a “willful disregard” is essential to make clear that a business cannot turn a blind eye to minors that use its platform. CCPA’s broader definition of “actual knowledge” to include “willful disregard” better ensures the protections it lays out to kids and teens are effective by covering the businesses it should. As a result, it is imperative this knowledge standard is clear in both the Act and the Agency’s regulations.

***We recommend that the Agency make clear the responsibilities of a business once it has actual knowledge that a consumer is under 16 years of age.*** Section 1798.120(c) provides:

Notwithstanding subdivision (a), a business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers between 13 and 16 years of age, or the consumer’s parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer’s personal information.

This implies that a business may continue to sell or share a consumer’s personal information until it has actual knowledge that the consumer is under the age of 16. It also implies that the business must stop selling or sharing such information until it obtains consent.

The Agency should make these two implications explicit in its modified proposed regulations. This is necessary guidance that would give businesses a better understanding of how to comply with the children and teens’ protections in the Act. Explicit guidance can help prevent businesses from unintentionally violating the Act because they were unsure of the specifics of compliance. We offer the following for consideration:

“Once a business has actual knowledge that a consumer is under 16, it must immediately stop selling or sharing personal information about the consumer. A business cannot resume selling or sharing personal information unless it has obtained consent from: (1) the

---

<sup>1</sup> See e.g. [Press Release, Federal Trade Commission, Google and YouTube Will Pay Record \\$170 Million for Alleged Violations of Children’s Privacy Law](#) (Sept. 4, 2019).

parent or guardian of consumers under the age of 13; or (2) consumers if they are between the age of 13 and 16.”

### **Comments to § 7070.**

***We recommend the Agency establish a specific time by when a business must inform parents or guardians of consumers under the age of 13 of their right to opt out of the sale or sharing of their personal information.*** Under section 7070(b), a business must inform the parent or guardian of consumers under 13 that they may opt-out of the sale or sharing of personal information on behalf of their child “when” a business receives consent to the sale or sharing of personal information. We believe that “when” suggests that the parent or guardian must receive this information at the same time or close in time to the business’s receipt of parental consent. Establishing a specific time frame in which the business must inform parents or guardians of the right to opt out emphasizes to businesses that they must not delay in providing this notice and gives them an easy-to-understand deadline. A required period of time would ensure parents and guardians receive this information in a timely manner while clarifying to businesses that they do not have to provide this information at the same moment they receive consent to the sale or sharing of personal information.

To make clear a business’ responsibilities under this section, we offer the proposed edits for consideration.

“~~When a business receives an affirmative authorization~~ **Within [a period certain] of receiving consent to the sale or sharing of personal information** pursuant to subsection (a), the business shall inform the parent or guardian of the right to opt out **of sale/sharing** and of the process for doing so on behalf of their child pursuant to section 7026, subsections (a)-(f).”

### **Comments to § 7071.**

***We recommend the Agency amend § 7071(b) again to make clear that businesses must inform consumers between the ages of 13 and 16 of their opt-out right when the opt-in request is received.*** In our August comments, we recommended that the Agency establish a specific timeframe by when a business must inform consumers between the age of 13 and 16 of their right to opt out of the sale or sharing of their personal information. Under section 7071(b) of the Act, when a business receives an opt-in request from consumers between the age of 13 and 16, the provision states the business must inform them of their right to opt-out “at a later date.”

The modified provision now states “...the business shall inform the consumer of their **ongoing** right to opt-out of sale/sharing at **any point in the future a later date...**” In its explanation of the modified proposed regulations, the Agency states that its revision of the subsection was intended to clarify that “businesses must notify consumers, at the moment the opt-in request is received, that the consumer has an ongoing right to opt-out of sale/sharing at any point in the future.” Unfortunately, the revision of the text still creates some confusion for businesses and consumers, which could result in businesses delaying when they notify consumers of their right to opt-out. Although “at

any point in the future" is intended to refer to the consumer being free to exercise their right to opt-out of sale/sharing at any time, it could also be misinterpreted to mean the business can, at any time the business chooses in the future, notify the consumer of the opt-out right.

To make clear that section 7071(b) requires businesses to inform consumers between the ages of 13 and 16 of their opt-out right when the opt-in request is received, we offer the proposed edits for consideration.

~~"When a business receives~~ **Within [a period certain] of a business receiving** a request to opt-in to the sale or sharing of personal information from a consumer at least 13 years of age and less than 16 years of age, the business shall inform the consumer of their ongoing right to opt-out of sale/sharing at any point in the future a later date and of the process for doing so pursuant to section 7026."

This proposed edit would clarify that businesses must inform consumers of their opt-out right in a timely manner.

Additionally, while the modified proposed regulations made revisions to section 7071(b), which pertains to a business' requirement to inform minors between the ages of 13 to 16 of their right to opt out, it did not make revisions to section 7070(b), which lays out the business' same obligation to parents or guardians of consumers under the age of 13. The Agency must specify in the modified proposed regulations the time frame in which businesses must inform both of these groups to clearly show they owe the same responsibility to both.

## **Conclusion**

Common Sense appreciates the Agency's work on these modified proposed regulations to implement the CPRA, and urges the Agency to take the steps recommended in these comments to revise and provide further clarity to the regulations pertaining to consumers under 16. Thank you for your consideration of these comments.

Respectfully submitted,

/s/ Jolina Cuaresma

Jolina Cuaresma, Senior Counsel, Privacy and Tech Policy  
Common Sense Media

/s/ Irene Ly

Irene Ly, Policy Counsel  
Common Sense Media

---

**From:** Crenshaw, Jordan [REDACTED]  
**Sent:** Monday, November 21, 2022 6:46 AM  
**To:** Regulations  
**Cc:** Quaadman, Tom  
**Subject:** CPPA Public Comment  
**Attachments:** 221118\_Comments\_CaliforniaPrivacyRightsAct\_CPRA.pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender [REDACTED]

To Whom It May Concern:

Please find attached the U.S. Chamber of Commerce's comments in response to the Proposed Modified Regulations.

Thank you.

Best,

**Jordan Crenshaw**

Vice President  
Chamber Technology Engagement Center  
U.S. Chamber of Commerce  
Direct [REDACTED] Cell: [REDACTED]



U.S. Chamber of Commerce

[www.americaninnovators.com](http://www.americaninnovators.com)

[REDACTED]



U.S. Chamber of Commerce

1615 H Street, NW  
Washington, DC 20062-2000  
uschamber.com

November 21, 2022

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

To Whom It May Concern:

***Re: Notice of Proposed Rulemaking, California Privacy Protection Agency; California Privacy Rights Act of 2020 (November 3, 2022)***

The U.S. Chamber of Commerce’s Technology Engagement Center (“Chamber” or “C\_TEC”) appreciates the opportunity to provide public comment on its Modified Proposed Rules to amend California’s privacy regulations to implement the California Privacy Rights Act (“CPRA”).<sup>1</sup> Consumers deserve strong privacy protections and innovative products as services. Businesses need certainty, uniformity, and protections against abusive litigation. It is for this reason that the Chamber supports national privacy legislation that does all these things. The California Privacy Protection Agency’s (“CPPA” or “Agency”) proposed rules will impact businesses beyond the borders of the Golden State. Therefore, we offer the following comments promoting consumer protection and business clarity that fall within the limits of CPRA.<sup>2</sup>

**I. The Agency Should Align the Consent Requirements in Section 7002 with the CPRA.**

Secondary uses of data are instrumental in serving consumers better as well as helping solve many of society’s greatest challenges and providing a public interest benefit.<sup>3</sup> For example, secondary data is being used to combat online fraud, expand financial inclusion, and examine social determinants of health. It is critical for these societally beneficial uses of data to continue to be reaped. This would allow flexibility while protecting consumers’ rights in this matter so as not to dry up the data pools necessary to achieve these positive goals of public safety and inclusion.

The Modified Proposed Regulations regarding the use of secondary data establishes separate standards for assessing the consumer’s reasonable expectations and whether a

---

<sup>1</sup> [https://cppa.ca.gov/regulations/pdf/20221102\\_mod\\_text.pdf](https://cppa.ca.gov/regulations/pdf/20221102_mod_text.pdf)

<sup>2</sup> The Chamber previously filed comments in August 2022 regarding the initial proposed rules for CPRA and continues to articulate the same concerns addressed therein at [https://americaninnovators.com/wp-content/uploads/2022/08/220819\\_Comments\\_CPRARegulationsNOPR\\_CPRA.pdf](https://americaninnovators.com/wp-content/uploads/2022/08/220819_Comments_CPRARegulationsNOPR_CPRA.pdf)

<sup>3</sup> [https://americaninnovators.com/wp-content/uploads/2020/01/CTEC\\_DataForGood\\_v4-DIGITAL.pdf](https://americaninnovators.com/wp-content/uploads/2020/01/CTEC_DataForGood_v4-DIGITAL.pdf)



disclosed purpose of processing is compatible with the context in which the personal information was collected. This creates potential confusion and gives the CPPA too much discretion to ignore disclosures made to consumers.

The Modified Proposed Regulations would require “consent...before collecting or processing the consumer’s personal information for any purpose” that is not considered “reasonably necessary and proportionate to achieve...the purposes for which the information was collection” or “...another disclosed purpose that is compatible with the context in which the personal information was collected...”<sup>4</sup> The Chamber urges the CPPA to align the regulations with the CPRA by clarifying that a business may use personal information for purposes that are compatible with any purpose disclosed at the time of collection.<sup>5</sup>

## II. The Proposed Global Opt-Out Mandate Exceeds the CPPA’s Statutory Authority.

Section 7025 of the Proposed Regulations mandates obligations on businesses who receive opt-out preference signals and to treat such signals as a verified request to opt-out. Specifically, Section 7025(b) states “[a] business that sells or shares personal information *shall* process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing.”<sup>6</sup> The CPRA does not authorize the CPPA to legislate this new mandate.

The CPRA provides companies with an option of one of two methods to honor a request by a consumer to opt-out of the “selling” or “sharing” of personal information. One method to honor a verified opt-out request is to post a “Do Not Sell or Share My Personal Information” link and if applicable, a “Limit the Use of My Sensitive Personal Information” link.<sup>7</sup> Alternatively, businesses do not need to offer such a link “*if* the business allows consumers to opt-out of the sale or sharing of their personal information and to limit the use of their sensitive personal information through an opt-out preference signal...”<sup>8</sup> The statute’s use of the word “*if*” makes it clear that CPRA treats responses to opt-out preference signals as voluntary. The voluntary nature of opt-out preference signals is further evidenced by other language such as “[a] business that *allows* consumers to opt-out of the sale or sharing of their personal information and to limit the use of their sensitive personal information pursuant to paragraph (1) may provide a link to a web page that enables the consumer to consent to the business ignoring the opt-out preference signal...”<sup>9</sup>

As many of the Chamber’s members operate nationwide including in the state of California, it is in the interest of both consumers and the business community to eliminate

<sup>4</sup> Modified Proposed Regulations § 7002(a),(e).

<sup>5</sup> [https://americaninnovators.com/wp-content/uploads/2022/08/220819\\_Comments\\_CPRARegulationsNOPR\\_CPRA.pdf](https://americaninnovators.com/wp-content/uploads/2022/08/220819_Comments_CPRARegulationsNOPR_CPRA.pdf)

<sup>6</sup> Proposed Regulations § 7025(b).

<sup>7</sup> CAL. CIV. CODE § 1798.135(a).

<sup>8</sup> *Id.* At § 1798.135(b)(1) (emphasis added).

<sup>9</sup> *Id.* At 1798.135(b)(2) (emphasis added).

confusion and potentially conflicting data rights. For this reason, Section 7025(b) should be revised to conform to CPRA and treat recognition of global opt-out preference signals as voluntary and not mandatory.

Giving businesses the flexibility with respect to recognizing a global opt-out preference signal, as envisioned by the statute, is important. There are many uncertainties regarding how such signals would be implemented, how businesses are to treat multiple global opt preference signals that could conflict, and how to ensure that such signals do not have anti-competitive consequences. There is currently no universal opt-out preference signal capable of effectively communicating a consumer's opt-out preferences to all websites, online platforms, or mobile applications. Universal opt-preference signals should be an optional method to honor opt-outs as outlined in the statute.

Moreover, the proposed regulations ignore important statutory requirements designed to ensure consumers make informed opt-out choices. In particular, the Agency should ensure that any global opt-out preference is free of defaults that presuppose consumer intent, is clearly described and easy to use, and does not conflict with other commonly used privacy settings. A mechanism that fails to accurately identify California residents and inform them of the specific privacy choices under the CPRA would not meet the statutory requirements for obtaining informed consumer consent.

### **III. Fair Enforcement Timelines**

CPRA requires the CPPA to finalize all implementing regulations by July 1, 2022—12 months prior to the date of CPRA enforcement.<sup>10</sup> Companies now run the risk of being in violation of the Act without receiving needed clarity for compliance because the Agency has not finalized all required rulemakings. This is even made more of a concern by the fact that California's exemption for business-to-business contact data and employee data will lapse at the end of the year.

The CPPA should delay both the effective and enforcement dates in light of the delayed rulemaking. CPPA should not retroactively enforce as well where it has failed to finalize regulations. The draft regulations establish a purely discretionary standard, which does not provide businesses with the needed time or certainty. At a minimum, there should be at least six months before the finalization of the implementing regulations and the effective date. Businesses are currently in the untenable position of trying to comply with the CPRA without finalized regulations.

### **IV. Conclusion**

The Chamber stands ready to work with you to ensure that the CPPA protects the laudable goals of giving consumers the right to access, correct, delete, and opt-out of sharing

---

<sup>10</sup> Cal. Civ. Code § 1798.185(d)

information among others. At the same time, we urge the Agency to pursue fair enforcement and carefully follow the statutory text which will provide the certainty needed for a thriving innovation economy.

If you have any further questions and need clarification, please contact me at

[REDACTED]

Sincerely,

[REDACTED]

Jordan Crenshaw  
Vice President  
Chamber Technology Engagement Center  
U.S. Chamber of Commerce

---

**From:** Cynthia Pantazis [REDACTED]  
**Sent:** Monday, November 21, 2022 7:02 AM  
**To:** Regulations  
**Subject:** CPPA Public Comment  
**Attachments:** Google Comments CCPA Modified Proposed Regulations - November 21, 2022.pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender [REDACTED]

Attached please find Google's comments on the California Privacy Protection Agency's proposed modifications to the draft California Consumer Privacy Act.

Thank you.

Cynthia Pantazis  
Director, State Policy  
Google LLC  
25 Massachusetts Avenue, NW  
Washington, DC 20001



November 21, 2022

**BY EMAIL**

California Privacy Protection Agency  
Attn: Brian Soublet  
2101 Arena Blvd.  
Sacramento, CA 95834  
[regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

Dear Mr. Soublet:

Please find below Google's comments on the California Privacy Protection Agency's ("Agency") proposed modifications to the draft California Consumer Privacy Act ("CCPA") regulations (hereinafter, "modified proposed regulations"). We thank the Agency and the representatives of the California Attorney General's office for the additional opportunity to comment on the modified proposed regulations.

**1. Introduction and General Considerations**

In our August 2022 comments regarding the proposed regulations implementing the California Privacy Rights Act ("CPRA"), we offered three overarching suggestions for the Agency to consider: (1) prioritize the prevention of consumer harms and promotion of privacy-protective business practices over establishing additional, prescriptive obligations; (2) wherever possible, seek to harmonize the CPRA with existing privacy regimes and other state privacy laws to facilitate consumer understanding and encourage development of consistent and privacy-protective business practices; and (3) ensure that the audit and enforcement provisions enable the Agency to punish violators, while taking into account the burden on law-abiding companies. We recognize that the modified proposed regulations take these comments into account in several areas, including helpful clarifications with respect to permissible processing and third party obligations. Our additional comments focus on the specific areas where the regulations could benefit from further clarity.

**2. Sec. 7002: Restrictions on the Collection and Use of Personal Information**

The Agency's revisions to this Section importantly acknowledge the role of privacy disclosures and a consumer's relationship with a business, as well as measures the business has taken to minimize the risk of consumer harm.

However, the modified Section 7002(b)(5) now provides that “the degree of involvement of service providers, contractors, third parties, or other entities in the processing is apparent to the consumer” is a consideration in whether data processing is consistent with a consumer’s reasonable expectations. This language could be understood to suggest that collection and processing performed by a service provider or contractor on a business’s behalf may somehow be less “expected”—and thus less likely to be lawful—than the same collection or processing undertaken by the business itself. This distinction is at odds with the text and structure of the CPRA, which provides that service providers and contractors operate pursuant to contract, on a business’s behalf and at its direction. A business’s choice, for example, to rely on routine cloud hosting services should not be understood to impact a consumer’s reasonable expectations around that data processing. This language could also have the undesirable effect of discouraging use of service providers and contractors, which are often better situated to provide privacy-protective services (such as fraud detection) on behalf of businesses. We agree that the degree of involvement of *third parties*—which by definition independently determine the purposes and means of processing personal information—is relevant to determining whether particular processing is consistent with the reasonable expectations of a consumer, but the same is not true of service providers and contractors.

To address this issue and avoid discouraging businesses from the routine industry practice of relying on service providers and contractors, we suggest striking the references to service providers and contractors in Section 7002(b)(5).

*Proposed Amendment:*

Sec. 7002(b): “The purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer(s) whose personal information is collected or processed. The consumer’s reasonable expectations concerning the purpose for which the personal information will be collected or processed shall be based on the following: . . .

(5): The degree to which the involvement of ~~service providers, contractors~~, third parties, or other entities in the collecting or processing of personal information is apparent to the consumer(s). 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 ~~third party service provider~~ if the consumer is not directly interacting with the ~~third party service provider~~ or the ~~third party service provider~~’s role in the processing is not apparent to the consumer.”

### **3. Sec. 7025(b): Technical Specifications for Opt-Out Preference Signals**

As described in more detail in our prior comments, the proposed regulations do not address the statutory obligation to “define the requirements and technical specifications for 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 and to limit the use or disclosure of the consumer’s sensitive personal information,” nor the topics that such regulations must address, such as how the opt-out choice must be presented, or that the opt-out preference signal is consumer-friendly, clearly represents a consumer’s intent, and does not conflict with other settings.

The modified proposed regulations have added a “JavaScript object” as an example of a commonly used format for opt-out signals. However, as with the prior reference to HTTP header fields, this addition does not provide companies with meaningful guidance or certainty around how to identify and honor legally valid opt-out signals, or ensure that signals meet the statutorily mandated elements.

The technical specifications and guidance mandated by the CPRA are vital for developers of these signals, for consumers seeking to choose and rely on them to exercise their rights, and for businesses that must honor them. Without these specifications or any process for the Agency to approve particular signals, the goals of the CPRA with respect to common, universal opt-out choices cannot be met, as it will lead to guesswork for consumers and businesses, conflicting signals, and post hoc enforcement actions. In order for these automated signals to serve the purpose of enabling consumers to opt-out in a seamless and predictable way, businesses must know which signals to look for and how to process them. In particular, as we noted in our prior comments, before requiring businesses to honor opt-out preference signals, the Agency should tell businesses which particular signals, formats, or tools are valid. Indeed, the new draft regulations implementing the Colorado Privacy Act (the “CPA Rules”) require the Colorado Department of Law to maintain a public list of Universal Opt-Out Mechanisms that companies must honor.<sup>1</sup> The Agency should adopt a similar approach to provide guidance and certainty as to which signals must be honored, or at minimum state with greater precision the criteria that make a signal, format, or tool qualify under the law, as the draft CPA Rules have done.

We urge the Agency to provide clarity on what signals are valid under the law and how companies are to respond to them at a technical level, and to clarify the processes by which the Agency will approve particular signals and ensure these processes are open and responsive to stakeholder feedback. As suggested in our prior comments, the Agency should delay enforcement of Section 7025 (and any provisions of the regulations or the CPRA relating to opt-out preference signals) until a reasonable time after the Agency has issued final regulations addressing these issues.

*Proposed Amendments:*

Strike Section 7025 of the proposed regulations in its entirety, as well as the associated notice requirements in Section 7011(e)(3)(F) and (G), until the Agency defines the requirements and technical specifications for opt-out preference signals.

---

<sup>1</sup> See CPA Draft Rules, Rule 5.07(A).

In the alternative, add a new subsection (h) to Section 7025 that provides: “(h) The Agency will not enforce this section 7025, nor any provisions of these regulations or the CCPA relating to opt-out preference signals until six months after the Agency has issued final regulations addressing requirements and technical specifications for opt-out preference signals pursuant to section 1798.185(19), Civil Code.”

Sec. 7011(e): “The privacy policy shall include ~~or facilitate readily available access to the~~ following information...

(3) An explanation of how consumers can exercise their CCPA rights and consumers can expect from that process, which includes the following: ...

~~(F) Explanation of how an opt-out preference signal will be processed for the consumer (i.e., whether the signal applies to the device, browser, consumer account, and/or offline sales, and in what circumstances) and how the consumer can use an opt-out preference signal;~~

~~(G) If the business processes opt-out preference signals in a frictionless manner, information on how consumers can implement opt-out preference signals for the business to process in a frictionless manner;”~~

#### **4. Sec. 7051(a)(5): Service Providers’ and Contractors’ Ability to Combine Personal Information**

As we outlined in our prior comments, the example in Section 7051(a)(5) of the proposed regulations appears to require contracts to prohibit a service provider or contractor from combining personal information received from, or on behalf of, one business with that received from, or on behalf of, another business “unless expressly permitted by the CCPA or these regulations.”<sup>2</sup> However, the proposed regulations do not expressly address the circumstances under which a service provider or contractor may combine data received from different businesses. As a result, the language of Section 7051(a)(5) may cast doubt on service providers’ and contractors’ ability to combine personal information collected across their business customers for *any* purpose, including wholly non-controversial purposes such as detecting and preventing fraud.

This result appears to be inadvertent, as it would be at odds with the text of the CPRA and other parts of the regulations expressly prohibiting only specific types of data combinations. The CPRA specifically contemplates that service providers and contractors should be able to combine personal information for business purposes other than as expressly prohibited in the CPRA, and requires the Agency to specifically address this in the regulations implementing the

---

<sup>2</sup> Modified Proposed Regulations § 7051(a)(5).



law.<sup>3</sup> However, the regulations fail to define such circumstances, and instead merely refer back to the statute.<sup>4</sup>

To address this potential confusion, we recommend that the regulations implement the CPRA's mandate to expressly confirm that service providers and contractors may combine consumers' personal information obtained from different sources for business purposes other than as prohibited in Section 1798.140(e)(6). Alternatively, the Agency should strike altogether from Section 7051(a)(5) the reference to combining data.

*Proposed Amendment:*

Sec. 7051(a)(5): "The contract required by the CCPA for service providers and contractors shall: [...] Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it Collected pursuant to a written contract with the business outside the direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations. For example, a service provider or contractor shall be prohibited from combining or updating personal information that it Collected pursuant to the written contract with the business with personal information that it received from another source or Collected from its own interaction with the consumer, **provided however that the service provider or contractor may combine personal information to perform any business purpose as defined in Civil Code section 1798.140(e), except, as provided in paragraph (6) thereof, providing advertising and marketing services shall not include cross-context behavioral advertising, and when providing such services, the service provider or contractor shall not combine the personal information of opted-out consumers that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or persons or collects from its own interaction with consumers unless expressly permitted by the CCPA or these regulations.**"

*Alternative Proposed Amendment:*

Revise Section 7051(a)(5) to strike the reference to combining personal information, as follows:

Sec. 7051(a)(5): "The contract required by the CCPA for service providers and contractors shall: [...] Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it Collected pursuant to a written contract with the business outside the

<sup>3</sup> See Cal. Civ. Code § 1798.140(ag)(1)(D) (stating that a "service provider may combine personal information to perform any business purpose as defined in regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) of this Section and in regulations adopted by the" Agency); *id.* § 1798.140(j)(1)(a)(iv) (stating the same with respect to contractors); *id.* § 1798.185(a)(10) (charging the Agency with issuing regulations "further defining the business purposes for which service providers and contractors may combine consumers' personal information obtained from different sources").

<sup>4</sup> See Modified Proposed Regulations § 7051(a)(5) (prohibiting service providers and contractors from combining personal information "*unless expressly permitted by the CCPA or these regulations*") (emphasis added); *compare* § 7050(b) (prohibiting service providers and contractors only from combining personal information in a narrower range of circumstances).

direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations. ~~For example, a service provider or contractor shall be prohibited from combining or updating personal information that it Collected pursuant to the written contract with the business with personal information that it received from another source or Collected from its own interaction with the consumer, unless expressly permitted by the CCPA or these regulations.”~~

## 5. Sec. 7051, 7052, and 7053: Requirements for Agreements with Third Parties and Service Providers

The modified proposed regulations include some limited changes to the contractual requirements for agreements that businesses maintain with third parties and service providers. In our prior comments, we recommend additional changes to make these requirements less prescriptive and avoid imposing lengthy and formulaic requirements for every contract with service providers and third parties.

Additionally, although Section 7053(a) provides that Section 7053 only applies to “a business that *sells or shares* (i.e., shares for cross-context behavioral advertising purposes) a consumer’s personal information with a third party” (emphasis added), the modified proposed regulations revise Section 7053(a)’s subsections to refer more broadly to personal information that these businesses “*make available*” to third parties. Similarly, Section 7052(a) now provides that a third party without a contract compliant with Section 7053(a) “shall not collect, use, process, retain, sell, or share the personal information that the business *made available to it.*” (emphasis added).

While these changes are not necessarily inconsistent with Section 7053(a)’s application to only *selling or sharing* of personal information by a business with a third party, the Explanation of Modified Text of Proposed Regulations (hereinafter, “Explanation of Modified Text”) contains potentially confusing language suggesting that the revisions were intended to make Section 7053 applicable to conduct broader than selling or sharing.<sup>5</sup> In particular, the Explanation of Modified Text references “more closely align[ing] the regulation with Civil Code § 1798.100(d)” as the reason for this change, but that Section of the CPRA is clearly limited to a business’s selling or sharing of personal information with a third party (as opposed to the broader “disclosure” of personal information to a service provider).

This reference appears to be an error, as “sharing” is a specific, defined term by the CPRA, which does not equate to mere disclosure.<sup>6</sup> We therefore recommend that the aforementioned

<sup>5</sup> See Explanation of Modified Text (noting that Sections 7052 and 7053 now use the phrase “‘made available to,’ which includes a business selling, sharing, *and otherwise making personal information available to a third party.*”) (emphasis added).

<sup>6</sup> Cal. Civ. Code § 1798.140(ah)(1) (defining “sharing” as “sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to a third party *for cross-context behavioral advertising*”) (emphasis added); (2) (enumerating specific examples that do not constitute sharing under the CPRA, including, for example, when “[a] consumer uses or directs the

language in the Explanation of Modified Text be clarified, or that the proposed regulations otherwise confirm that Sections 7053 and 7052 only apply to “[a] business that sells or shares a consumer’s personal information with a third party.”

*Proposed Amendments:*

Strike Sections 7051 and 7053 in their entirety, or alternatively edit Sections 7051(c) and 7053(c) as follows:

7051(c): “A person who does not have a contract that complies **in material respects** with subsection (a) is not a “service provider” or a “contractor” under the CCPA. For example, a business’s disclosure of personal information to a person who does not have a contract that complies **in material respects** with these requirements may be considered a sale for which the business must provide the consumer with the right to opt-out of sale/sharing.”

7053(c): “A ~~third-party~~ **first party shall not sell or share personal information with a third party unless it has that does not have** a contract **with the third party** that complies **in material respects** with subsection (a) ~~shall not collect, use, process, retain, sell, or share the personal information received from the business.~~”

Revise the Explanation of Modified Text or proposed regulations to clarify that that Sections 7053 and 7052 only apply to “[a] business that sells or shares a consumer’s personal information with a third party.”

## **6. Sec. 7004: Dark Patterns**

Our prior comments recommended a less prescriptive approach to rules around dark patterns, which as currently framed are likely to result in more formulaic notices that diminish consumer understanding and lead to notice blindness and information “fatigue.” The modified proposed regulations include modest revisions to Section 7004, but largely maintain the prescriptive approach. We continue to recommend that the proposed regulations be modified to remove the detailed prohibitions, permitting businesses more flexibility in how they communicate with consumers in a particular context.

The need for flexibility is made clearer by the recently-issued CPA Draft Rules, which include additional, prescriptive rules and examples that diverge from the Agency’s proposed approach. It would be particularly challenging for businesses to simultaneously comply with different, highly detailed rules in multiple states for user interfaces that are utilized in multiple jurisdictions.

The Agency should also confirm that a dark pattern must have the “*substantial effect of* subverting or impairing user autonomy, decision-making, or choice.” This is an express requirement of the statutory definition, and an area that the CPRA contemplates be “further

---

business to; (i) intentionally disclose personal information; or (ii) intentionally interact with one or more third parties”).

defined by regulation.”<sup>7</sup> However, the language of the modified proposed regulations, in Section 7004(b), states that *any* user interface that does not comply with the highly detailed and specific design components set forth in Section 7004(a) may be deemed a “dark pattern.” Moreover, confirming that a dark pattern must have the “substantial effect of subverting or impairing user autonomy, decision-making, or choice” would more closely harmonize the modified proposed regulations with the CPA Draft Rules, which presents a similar standard, then outlines “principles [to] . . . be considered” when determining whether a dark pattern exists (without suggesting that a bare violation of these principles could constitute a dark pattern, regardless of the standard).<sup>8</sup>

Finally, by deleting the prior reference to a consumer’s right to opt-out of the sale or sharing of their personal information in Section 7004(a)(2)(C), the modified proposed regulations create additional confusion by invoking an example of a company seeking consent to *use* a consumer’s personal information – which is rarely addressed by the CPRA’s requirements – rather than overcoming a prior opt-out from the sale or sharing of the consumer’s information. We therefore recommend that the Agency strike Section 7004(a)(2)(C) in its entirety or, in the alternative, reinsert the language that ties the example to a method for opting out of sales or sharing.

In addition to the proposed redlines we put forth in our prior comments, which we reiterate here, we propose the following additional amendments to implement our suggestions above:

*Proposed Amendments:*

Sec. 7004(b): “A method that does not comply with subsection (a) ~~may~~**shall** be considered a dark pattern **if the method has the substantial effect of subverting or impairing user autonomy, decision-making, or choice**. Any agreement obtained through the use of dark patterns shall not constitute consumer consent. For example, a business that uses dark patterns to obtain consent from a consumer to sell their personal information shall be in the position of never having obtained the consumer’s consent to do so.”

Strike Sec. 7004(a)(2)(C) in its entirety.

## **7. Sec. 7301 - 7303 and 7304: Agency Audits and Enforcement**

The modified proposed regulations do not include any revisions to the audits provisions in Section 7304, and only modest revisions to the enforcement provisions. We urge the Agency to reconsider the proposed changes we put forth in our prior comments, including the specific

---

<sup>7</sup> *Id.* § 1798.140(l) (emphasis added).

<sup>8</sup> See CPA Draft Rules, Rule 7.09(A) (defining dark patterns as having “the substantial effect of subverting or impairing user autonomy, decision making or choice, or unfairly, fraudulently, or deceptively manipulating or coercing a Consumer into providing Consent”); (B) (delineating “principles [to] . . . be considered when designing a user interface or a choice architecture”).

redlines we proposed, to provide appropriate safeguards and ensure due process in such audits and any probable cause proceedings resulting from enforcement actions.

\* \* \* \* \*

We appreciate the opportunity to provide comments on the proposed regulations.

Sincerely,



Cynthia Pantazis  
Director, State Policy

---

**From:** Edwin Portugal [REDACTED]  
**Sent:** Monday, November 21, 2022 7:15 AM  
**To:** Regulations  
**Cc:** Matt Kownacki; Danielle Arlowe  
**Subject:** CPPA Public Comment on modified text of proposed regulations  
**Attachments:** AFSA comment letter - CA CPPA 2022 modified privacy rulemaking.pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear Mr. Soublet,

Attached is a letter from the American Financial Services Association commenting on the California Privacy Protection Agency's modifications of the proposed regulations implementing the CPRA. Thank you for the opportunity to provide feedback on the rules. Please let us know if you have any questions.

Best,  
Edwin



**Edwin Portugal**  
*Manager, State Policy & Regulatory Affairs*



November 21, 2022

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

**Re: Comments on modified text of rules implementing the California Privacy Rights Act of 2020**

Dear Mr. Soublet:

On behalf of the American Financial Services Association (“AFSA”),<sup>1</sup> thank you for the opportunity to provide comments on the California Privacy Protection Agency’s (“Agency”) November 3 modifications of proposed rulemaking to implement the California Privacy Rights Act of 2020 (CPRA). AFSA members share the state’s goal of protecting the privacy of consumers, promoting understanding by consumers of the personal information about them that is collected, sold, and shared for a business purpose, and guarding personal information from unauthorized access. We appreciate the Agency’s consideration of our previous comments and look forward to further engagement throughout the rulemaking process.

**Enforcement Delay**

The CPRA required that finalized regulations be completed by July 1, 2022, to provide businesses with enough time to comply before January 1, 2023, when the CPRA becomes operative, and before enforcement begins six months later, on July 1, 2023. As we discussed in previous comments, the rulemaking timeframe leaves businesses with very little time, if any, to alter operational practices to comply with the law. We appreciate the Agency’s recognition of these challenges through its inclusion of § 7301(b):

As part of the Agency’s decision to pursue investigations of possible or alleged violations of the CCPA, the Agency may consider all facts it determines to be relevant, including the amount of time between the effective date of the statutory or regulatory requirement(s) and the possible or alleged violation(s) of those requirements, and good faith efforts to comply with those requirements.

While we believe this section is a step in the right direction, we respectfully request stronger assurances that a company’s good faith effort to comply with the regulations will be considered in enforcement decisions. Accordingly, we request that the rules be modified to instead read: “the Agency *must* consider all facts...”

---

<sup>1</sup> Founded in 1916, the American Financial Services Association (AFSA), based in Washington, D.C., is the primary trade association for the consumer credit industry, protecting access to credit and consumer choice. AFSA members provide consumers with many kinds of credit, including direct and indirect vehicle financing, traditional installment loans, mortgages, payment cards, and retail sales finance. AFSA members do not provide payday or vehicle title loans.

## **Employee and B2B Data Exemption**

The California Privacy Rights (CPRA) extends the CCPA’s partial exemption of employee and business contact data until January 1, 2023. The expiration of the exemptions will create unintended consequences and compliance problems as employees, job applicants, employers and individuals serving other businesses in a service provider are left without further guidance and clarity regarding the interplay between the CPRA and employment laws. Most of the rights under the CPRA either are already addressed or do not make sense in the employment or B2B context, and neither the CPPA nor the California Attorney General has provided businesses with any guidance or draft regulations concerning the treatment of such data. We request that the Agency consider making the exemptions permanent or extend them to at least January 1, 2024, to allow for additional time to comply, if the legislature fails to take steps to extend them. Absent this exemption, we request that the Agency issue guidance and provide more clarity regarding CPRA obligations with respect to employee and B2B data.

## **Business Purpose Disclosures**

Section 7051(a)(2) requires businesses to identify, in each service provider or contractor agreement, the specific business purpose for which personal information is disclosed, which goes beyond the statute’s obligations. Section 7053(a)(1) of the draft regulations requires the same information for third party agreements, which also goes beyond the statute’s requirements and is not feasible. As currently written, this would require an impracticable amount of contract remediation to update executed contracts with this information. We request that these sections be removed from the final rules to align with the content of the statute.

## **Use of Sensitive Personal Information**

In some sections, the draft regulations contravene and narrow the scope of the statutory language, effectively disregarding Section 1798.121(a)-(b) of the CPRA, which permits a business to use a consumer’s sensitive personal information (SPI) for uses that are “necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services,” even after receipt of a consumer’s request to limit. While the regulations attempt to define permissible uses of Sensitive Personal Information in Section 7027(m), the eight use cases listed do not encompass all those uses of Sensitive Personal Information that may be “necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services.”

For example, section 7014(h) of the draft regulations would require consumer consent to disclose SPI outside collected at a time when a business did not have a notice of right to limit posted, except for the eight uses defined in Section 7027(m). As a notice of right to limit is not required until January 1, 2023 (and only if the business is collecting SPI for the purposes of inferring characteristics), any personal information collected prior to January 1, 2023, absent consumer consent, may not be used for any purpose other than one of the eight limited purposes defined by Section 7027(m). Similarly, in Section 7027(g)(1), the draft regulations require that, upon receipt of a request to limit, a business must cease to use and disclose SPI for any purpose other than the eight purposes listed in Section 7027(m).



Accordingly, we respectfully reiterate our request in our last letter that the Agency reconsider such narrowly defined uses or add an additional subsection to section 7027(m) allowing “any other acts or practices that may be necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services.”

### **Notice at Collection Online**

Section 7012(f) requires a business that collects personal information online to provide the notice at collection by providing a “a link that takes the consumer directly to the specific section of the business’ privacy policy that contains the information required in subsection (e)(1) through (6).” The section continues by stating that directing the consumer to the beginning of the privacy policy or to any other section without the required information will not satisfy the notice at collection requirement. We believe that this requirement is overly prescriptive, burdensome, and impracticable. For example, the information required in subsection (e)(1) through (6) may not be contained in the same section, and therefore may not be available at a single link, as maintained by the rule. We respectfully request that this requirement to link to a specific section be removed.

### **Downstream Notification of Opt-Out Requests to All Third Parties**

Section 7026(f)(2) requires a business to notify all third parties to whom the business has sold or shared a consumer’s personal information of a consumer’s request to opt-out of sale/sharing and to forward the consumer’s opt-out request to “any other person with whom the person has disclosed or shared the personal information.” Both requirements go beyond the requirements of the statute and would be technically challenging at the device level (whether in connection with a one-off device interaction or in response to a global privacy control). Further, the requirement to forward a consumer’s request to any person with whom the person has disclosed or shared the information does not take into consideration lawful disclosures to service providers, contractors, law enforcement, government agencies, or disclosures to other businesses or individuals pursuant to an explicit request or direction from the consumers to make the disclosure. These requirements go beyond the statute and are operationally difficult or impossible due to technological and practical limitations. We respectfully request that the Agency remove this requirement.

### **Archived or Backup Systems**

Section 7022(b)(1) requires businesses to delete a consumer’s personal information from its existing systems except “archived or back-up systems,” seemingly indicating that requests to delete do not trigger a requirement to delete personal information on archived or back-up systems. To the contrary, Section 7022(d) states that a business that stores any personal information on archived or back-up systems “may delay compliance with the consumer’s request” until the archived or back-up system is “restored to an active system or is next accessed or used for a sale, disclosure, or commercial purpose.” We request that the Agency clarify its position on deletion of information on archived or backed up systems. Is a business never required to delete personal information stored on archived or back-up systems (as long as it remains on such archived or back-up systems), or does a business have a requirement to delete personal information on archived or stored systems, with the understanding that requirement is not triggered unless, or until, a business activates that system or accesses, sells, discloses, or uses such data for a commercial purpose? Additionally, does “access” include de minimis, temporary,

or transient access for maintenance, information security, fraud, system improvement, and other purposes that do not require length or permanent access nor use or disclosure of personal information outside of the limited purposes mentioned?

### **Due Diligence**

Section 7051(c) and Section 7053(b) state that “[w]hether a business conducts due diligence of its” service providers, contractors, or third parties “factors into whether the business has reason to believe” the service provider, contractor, or third party is using personal information in violation of the CCPA/CPRA. Further, both provisions cite an example where a business that never enforces the terms of its contract nor exercises its rights to audit or test might not be able to rely on the defense that it did not have reason to believe that the service provider, contractor, or third party intended to use the personal information in violation of the CCPA. The provisions go beyond the statute and shift nearly all service provider, contractor, and third party liability to the business. Moreover, the provisions do not discuss what level of due diligence is required to prevent the shifting liability. We respectfully request that the Agency strike out or amend and clarify these provisions such that businesses know what level of due diligence is required to prevent the shifting liability.

### **Topics Unaddressed by the Proposed Rules**

Section 1798.185(a)(15) of the California Civil Code requires the Agency to issue rules governing risk assessments that businesses covered under the CPRA must submit to the Agency. The proposed regulations do not provide any guidance on the structure or frequency of these assessments. Additionally, Section 1798.185(a)(16) of the California Civil Code requires the Agency to issue regulations governing access and opt-out rights regarding a business’ use of automated decisionmaking technology. Many businesses use automated tools to conduct their businesses efficiently and eliminate bias in decisionmaking. The rules do not provide clarity over the use of these technologies as required by the statute.

Thank you in advance for your consideration of our comments. If you have any questions or would like to discuss this further, please do not hesitate to contact me at [REDACTED]

Sincerely,

[REDACTED]  
 Matthew Kownacki  
 Director, State Research and Policy  
 American Financial Services Association

---

**From:** Dylan Hoffman [REDACTED]  
**Sent:** Monday, November 21, 2022 7:14 AM  
**To:** Regulations  
**Cc:** Lia Nitake  
**Subject:** CPPA Public Comment - TechNet Comments on Modified CPRA Regulations  
**Attachments:** FINAL 2nd Round TechNet CPRA Comments.11.21.22.pdf

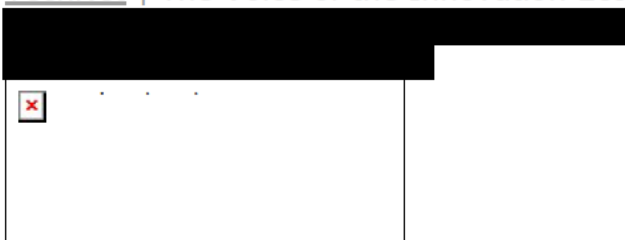
**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender [REDACTED]

Hi,

Please find TechNet's comments on the modified CPRA regulations attached. Let me know if you have any questions.

Best,

--  
Dylan Hoffman  
Executive Director | California & the Southwest  
[TechNet](#) | The Voice of the Innovation Economy





**25<sup>th</sup>**  
ANNIVERSARY

TechNet Southwest | Telephone 505.402.5738  
915 L Street, Suite 1270, Sacramento, CA 95814  
www.technet.org | @TechNetUpdate

November 21, 2022

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

**Re: TechNet Comments in Response to 15 Day Comment Period on Modified Regulations Under the California Privacy Rights Act of 2020**

Dear Mr. Soublet,

TechNet appreciates the opportunity to provide additional comments and feedback to the California Privacy Protection Agency as part of the formal California Privacy Rights Act (CPRA) rulemaking process.

TechNet is the national, bipartisan network of innovation economy CEOs and senior executives. Our diverse membership includes dynamic American businesses ranging from revolutionary start-ups to some of the most recognizable companies in the world. TechNet represents over five million employees and countless customers in the fields of information technology, e-commerce, sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

As noted previously, TechNet members support many of the privacy concepts within CPRA, such as a robust compilation of consumer rights like access, correction, deletion, transparency, and consumer choice, and we believe our suggestions enhance these rights, allow them to be accessed consistently across state lines, and allow for businesses to comply with clear and dependable guidelines for consumer privacy protections. We also appreciate some of the changes made to ease implementation, including changes made to third party notification requirements.

Based on the latest modified regulations we have additional comments and suggestions that we believe will help ensure effective compliance from companies and that consumers are able to easily exercise their rights under the CPRA.

**§ 7002. Restrictions on Collection and Use of Personal Information**

We appreciate that the modified regulations have removed the originally proposed "average consumer" standard that was not found in the statute and was going to lead to ambiguity in implementation. We remain concerned, however, that modified section 7002 creates confusion by creating a dual "reasonable expectations of consumer" standard based on either (1) a multi-factor test that underweights the

importance of disclosures or (2) compatibility of purpose based on the same flawed multi-factor test. The more appropriate focus of section 7002 limitation is on the reasonable expectations of consumers based on compatibility with a disclosed purpose. This appropriately allocates the value of disclosures in framing reasonable consumer expectations and ensures consistency in outcomes from that requirement. With respect to the latter, we note that as currently framed, the multi-factor analysis risks allowing the Agency to supplant its judgment for that of the business and even risks turning the California framework from a notice and opt-out jurisdiction into an opt-in regime, which the statute does not authorize the Agency to do. Instead, the Agency should amend the modified regulations to clarify that a business's collection and processing of personal information should be reasonably necessary and proportionate to achieve the (1) reasonable expectations of consumers consistent with the disclosed purposes for which the information was collected or processed or (2) another compatible purpose.

Proposed section 7002(a) of the draft regulations states that a business's collection of personal information must be "reasonably necessary and proportionate", while proposed section 7002(b) requires the purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer." This creates significant ambiguity since a business, consumer, and regulator may differ on the "reasonable expectations of a consumer", and it transforms the CPRA's transparency requirements into a nullity – even if a business is transparent, that simply isn't enough.

Injecting the "consumer expectations" standard, instead of the plain language of CPRA, leads to value judgments that will disfavor innovation and lead to inconsistent enforcement. The factor tests are subjective and almost impossible to apply to the complex technical processing that powers the internet, mobile apps, and connected devices. It also threatens to prohibit even otherwise legally permissible processing, such as creating new services or improving existing services. The highly open-ended nature of these requirements would place businesses in a constant state of uncertainty regarding whether they are in compliance. This would also be problematic for consumers, given that a highly complex and open-ended framework would leave consumers with a lack of clarity regarding expectations for how their personal information will be collected, used, retained, or shared. Moreover, it gives too little weight to disclosures, which are only one factor to be considered even though disclosures inextricably influence a consumer's reasonable expectations.

As one example of the confusing nature of the factor test, proposed section 7002(b)(5) should not include service providers or contractors because it is an irrelevant factor into a consumer's reasonable expectations. 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. We suggest removing this factor.

We suggest striking the “consumer expectations” standard as used in proposed section 7002(b) as well as the accompanying factor test. The Agency should instead revise the regulations to state that any collection should be reasonably necessary and proportionate and not materially inconsistent with the disclosed purposes of the collection.

### **§ 7004. Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent**

As we’ve stated previously, we agree with the intent of proposed section 7004, which is to ensure that consumers are appropriately presented with methods to submit their rights requests. However, the proposed symmetry choice standard for a dark pattern is overly broad and the latest modifications do not resolve the workability issues.

In order to ameliorate some of these issues we suggest the following revisions. (TechNet additions in **bold underline**, deletions in ~~strikethrough~~)

Amend proposed section 7004(a): “Except as expressly allowed by the CCPA and these regulations, businesses shall **make reasonable efforts** to design and implement methods for submitting CCPA requests and obtaining consumer consent that incorporate the following principles.”

Amend proposed section 7004(a)(2): “Symmetry in choice. 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.”

Amend proposed section 7004 (c): “A user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice. A business’s intent in designing the interface is not determinative in whether the user interface is a dark pattern, but a factor to be considered. **If a business can show that it had a process for reviewing user interfaces for dark patterns, this may weigh against establishing a dark pattern.** If a business did not intend to design the user interface to subvert or impair user choice, but the business knows of and does not remedy a user interface that has that effect, the user interface may still be a dark pattern. Similarly, a business’s deliberate ignorance of the effect of its user interface may also weigh in favor of establishing a dark pattern.”

## **§7025. Opt-Out Preference Signals**

The modified regulations' continued mandate that businesses honor global opt-outs is contrary to the text of CPRA, exceeds the Agency's rulemaking authority, and fail to address the specifications and requirements in the statute for opt-out signals.

We encourage the Agency to use the rulemaking to help develop standards for the still nascent concept of a global opt-out option or signal. At this time there is significant uncertainty for businesses about how to honor such signals. It is critical to develop interoperable principles, standards, and specifications to address the creation, implementation, ubiquity, and limitations of a global opt-out signal.

First, and most critically, the proposed regulations interpret the preference signals to be mandatory, despite clear statutory text that businesses have an option to either comply with the requirements for a Do Not Sell or Share link pursuant to Section 1798.135(a) *or* allow consumers to opt-out through an opt-out preference signal. *See*, Section 1798.135(b). The Agency does not have the authority to override the statute.

Moreover, the Agency achieves its interpretation that opt-out preference signals are mandatory through a strained interpretation of the CPRA that is further designed to obviate the clear statutory intent to create an option. To arrive at its interpretation that honoring the signals is mandatory, the Agency proposes an interpretation of the CPRA that would make the placement of the Do Not Sell or Share Links on a website optional if a business honors an opt-out signal in a "frictionless manner." Not only does this contradict the statute, but it is largely unachievable. For example, the draft regulations state that a business can only process the signal in a frictionless manner if it allows the preference signal to fully effectuate the consumer's request without requesting more information from the consumer. However, proposed section 7025(c)(2) plainly states that a business cannot require a consumer to provide this information. As a result, browser-based opt-out signals can't be honored in a frictionless manner because a business will not be able to connect that signal to a known consumer without additional information. The certainty of that outcome nullifies the interpretation of the "option" by the agency, which the statute expressly offers. This exceeds the agency's authority.

Secondly, the proposed regulations do not address the requirements and specifications set forth by the CPRA. The proposed regulations are silent on the requirements and fail to define any technical specifications that the statute directs the agency to ensure are met with respect to any opt-out signal. *See*, Section 1798.185(a)(19)(A)(i)-(vi). The limited information in the proposed regulations – stating only that the signal must be in a commonly used format such as an HTTP header – does not give businesses useful guidance concerning which signals they should look for, much less the technical means businesses should use to honor such signals. Rather than expanding on how an opt-out preference signal can meet these

statutory criteria, the proposed regulations issue a mandate for any such signal that meets two criteria created by the Agency rather than the statute. Neither of the two Agency-created criteria meet any of the statutory specifications for opt-out preference signals. Indeed, the second criterion created by the Agency directly contradicts the statutory standards in a number of ways. See, Proposed Section 7025(b). As just one example, it would wrongly allow a signal even if it fails to “clearly represent a consumer’s intent” by permitting the opt-out without any disclosures about the parameters of the opt-out right in California (including any limitations to this). This contravenes Section 1798.185(a)(19)(A)(ii) and (iii). As a result, if finalized as proposed, the regulations would allow signals that are non-compliant with the statutory standards. Moreover, by bypassing this, the regulations are creating two rules for consent: one for opt-out signals and one required by businesses. Not only does this not make sense, but it risks consumer confusion.

Without clarity on which signals are valid under the law and how companies are supposed to respond to them at a technical level, the goals of the CPRA with respect to universal opt out choices will not be met. Without that certainty, businesses’ potential liability for violations of the law will depend on guesswork regarding which signals they should honor, how to look for such signals, and how to honor them. That guesswork, in turn, is certain to frustrate user choice and to create chaos when signals conflict or are incompatible. The approach of the proposed regulations, moreover, is likely to result in the Agency expending substantial resources in fleshing out what signals must be honored and how through post hoc enforcement actions. The better approach, and the approach that is prescribed by the law, is for the Agency to provide that certainty upfront.

We strongly encourage the agency to ensure that the regulations address how opt-out signals can comply with the statutory requirements, as contemplated in the CPRA’s grant of rulemaking authority. The Agency should tell businesses that decide to utilize a global opt out option which particular signals, formats, or tools are valid, by reviewing nominated tools and determining which ones qualify.

### **§ 7050. Service Providers and Contractors**

First, 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 the 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 businesses, 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 and it is hashed, helps them reach their own customers in a privacy-protective way, effectively and efficiently. 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 in the US, and global, digital market as against their competitors outside of the State.

This section attempts to categorically ban certain practices for service provider or contractor relationships, which goes well beyond the Agency's statutory authority. The CPRA details the required elements for contracts with service providers and contractors. As long as a contract includes those elements, the Agency has no statutory basis on which to declare that the relationship is nevertheless a "third party" one.

This example contradicts the statute and raises new questions and uncertainty for businesses beyond those called out in the example. We suggest striking the example.

Finally, proposed section 7050(e) creates a disproportionate and compounding penalty where a business fails to have the required contract in place. Designating a service provider as a third party would not accurately reflect the business relationship and imposes compounding penalties by also likely necessitating a violation of the sale opt out (which would not apply to service provider relationships). The violation of the contract provision, standing alone, would be a sufficient penalty. We suggest removing the penalty in this section.

### **§§ 7051. Contract Requirements for Service Providers and Contractors, 7053. Contract Requirements for Third Parties**

First, proposed section 7051(a)(3) is overly prescriptive and fails to consider how businesses execute contracts while providing no additional protections to consumers. This provision requires that the section of a contract that specifies the purposes of processing include the prohibition against using the data for other

purposes. This level of prescription is unnecessary and this section should be removed. A business should be able to satisfy its obligations so long as the contract contains both requirements.

Additionally, proposed section 7051(a)(5) of the proposed regulations prohibits a service provider or contractor from combining personal information received from, or on behalf of, one business with that received from, or on behalf of, another business "unless expressly permitted by the CCPA or these regulations." The regulations further allow the combination of data for certain limited internal purposes and for fraud prevention. The limits on combining data appears to contradict broad permitted uses in 7050(b).

The Agency should strike this reference to combining data, or else modify Section 7051(a)(5) to make clear that that a service provider or contractor may combine or update personal information received from, or on behalf of, the business for the same business purposes for which they may use personal information. Alternatively, the Agency should revise Section 7051(a)(5) to align with the CCPA's definitions of "service provider" and "contractor," clarifying that service providers and contractors may combine data received from, or on behalf of, different clients for "business purposes" as defined by the CCPA, provided that where they are providing advertising and marketing services, they do not do so for cross-context behavioral advertising purposes, nor combine the personal information of opted-out users with other personal information.

Regarding proposed sections 7051(c) and 7053(b) of the draft regulations, we caution the Agency against creating a de facto requirement that businesses audit the data practices of their service providers and contractors regularly. See, section 7051(a)(6),(e). Proposed sections 7051(c) and 7053(b) create a de facto requirement that a business must conduct due diligence and audits on its service providers, contractors, and third parties. The proposed regulations require businesses to include extremely prescriptive provisions for all agreements with service providers and third parties. Failure to address all of these provisions (ten requirements in service provider agreements and six in contracts with third parties) would subject the business to substantial penalties, even for trivial missteps. For example, under proposed section 7051(c), a business could arguably be deemed to have "sold" personal information to another business without the corresponding notice and opt out even when the disclosure is made pursuant to a contract that provides that the recipient is a service provider to the disclosing business, simply because the contract does not meet every one of the ten elements mandated by subsection (a) of the same section.

The statute already addresses core requirements for service provider agreements (see Section 1798.140(ag)) and does not instruct the Agency to issue regulations concerning third-party agreements. Proposed sections 7051 and 7053 of the draft regulations create an onerous compliance regime for businesses with little to no

corresponding benefit to consumers. To the extent the Agency promulgates regulations on when the exemption in §1798.145(i) applies, they should be limited to factors that affirmatively indicate that the external party is violating its obligations—and not impose additional burdens on a business to confirm the absence of violations.

While a requirement for vendor due diligence makes sense, the suggestion that reasonable privacy vendor due diligence *mandates* ongoing manual reviews, automated scans, technical testing, and audits once every twelve months is unduly burdensome. First, the regulation does not take into account the risk associated with the service provider. Nor would this one-size-fits-all requirement make sense in practice. Rather, the regulations should clearly state that a business has an obligation to examine the vendor's practices if it has reason to believe there is a violation. Even the suggestion of what reasonable due diligence requires (i.e., stating in the regulations that audits, manual reviews, etc. "may" be required) will turn those suggestions into the de facto standard and increase the burden on businesses considerably.

Audits are resource-intensive exercises that are not warranted for most providers on a regular basis, absent indications that personal information is not managed appropriately. Third-party audits are burdensome and expensive, making a mandate inappropriate as the burden and expense would be disproportionate to any downstream consumer benefit, and the result would likely be increased consumer costs. Instead, businesses should be incentivized to take reasonable measures to oversee service providers' compliance with contractual requirements.

Similarly, a business's reasonable measures to oversee compliance by a third party with contractual requirements should be sufficient to protect it from liability for that third party's mismanagement (§7053(e)). If a business has a contract with a third party that separately controls collection of consumer personal information, it should not be required to identify this party upon collection. This requirement would be burdensome and cause consumer confusion, and it is only necessary if the business will use data for different purposes (§ 7012(e)(6),(g)).

We additionally suggest amending this section to include trusted privacy programs as reasonable privacy vendor due diligence. The CPRA requires businesses to take reasonable and appropriate steps to conduct due vendor diligence and utilizing existing accountability mechanisms or national industry self-regulation programs can be a cost-effective method to do so. If a business were to engage a service provider, contractor, or third party that utilizes a trusted privacy program, proof of such certification should be sufficient to ensure due diligence by the business as prescribed by section 7053(b). Therefore, we suggest sections 7051(a)(7), 7053(a)(4), and 7053(b) be amended to include trusted privacy programs as reasonable privacy vendor due diligence that facilitates businesses to oversee service providers' and contractor's compliance with contractual requirements.

Finally, proposed section 7053 seems to require for an additional set of scenarios that were not included in the CPRA. Section 1798.100 (d) of the CPRA sets requirements for an agreement between a business that collects and sells or shares personal information, and the recipient third party. On its face, this does not apply to a business that does not itself collect personal information, but merely allows a third party to collect personal information. Section 1798.100 (d) only applies to a business that *first* collects and *then* sells or shares personal information. In the example of browsing cookies, the business does not collect and then sell or share the personal information, the business only sells or shares when it allows a third party to collect the personal information. In other words, with cookies, the business "sells or shares" but does not "collect and sell or share." The proposed section 7053 eliminates that distinction.

We suggest section 7053 be amended with the following (TechNet additions in **bold underline**, deletions in ~~strikethrough~~): A business that ~~sells or shares~~ **collects** a consumer's personal information **and sells or shares that information** with a third party shall enter into an agreement with the third party that..."

### § 7015. Alternative Opt-Out Link

Under the current CCPA regulations, section 7013(f), the opt-out icon "may be used in addition to posting the notice of right to opt-out, but not in lieu of any requirement to post the notice of right to opt-out or a 'Do Not Sell My Personal Information' link". Under the draft regulations, section 7013(f) has been removed, and the opt-out icon is now moved to proposed section 7015(b) with the requirement to use the icon if the business chooses an alternative opt-out link. The business is required to title the link, "Your Privacy Choices" or "Your California Privacy Choices". We suggest maintaining the permissive standard from CCPA regulations section 7013(f) with the following change. (TechNet additions in **bold underline**, deletions in ~~strikethrough~~)

Amend proposed section 7015(b): "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."

### § 7023. Requests to Correct

The right to delete and right to correct can be important tools for consumers to control their information and when necessary to correct inaccurate information that may be preventing them from accessing housing, job or educational opportunities. But outside of those defined areas it could impose a significant burden on

businesses. New compliance obligations for consumers' rights to delete or correct their personal information should be justified with clear benefits to consumers.

Proposed section 7023(h) requires a business to provide an explanation as to why it believes a request to correct is fraudulent or abusive. Businesses should not be required to explain to fraudsters or bad actors seeking to abuse our sites how to evade our fraud and abuse detection mechanisms. This requirement should be stricken; however, the following change would help mitigate the risk of abuse. (TechNet additions in **bold underline**, deletions in ~~strikethrough~~)

"A business may deny a request to correct if it has a good-faith, reasonable, and documented belief that a request to correct is fraudulent or abusive. The business shall inform the requestor that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent or abusive- **provided however, that the business shall not be required to provide any information to the requestor the disclosure of which could potentially reveal how to subvert the business's authentication, fraud prevention, or other processes designed to ensure that personal information is not improperly corrected.**"

We also suggest that proposed section 7023(k) should include a reasonableness standard as follows (TechNet additions in **bold underline**):

"Failing to consider and **use reasonable efforts to** address the possibility that corrected information may be overridden by inaccurate information subsequently received from a data broker may factor into whether that business, service provider, or contractor has adequately complied with a consumer's request to correct."

## **§ 7012. Notice at Collection of Personal Information**

Proposed section 7012(f) requires that if a business collects information from a consumer online, the notice at collection must take the consumer *directly* to the *specific section* of the business's privacy policy that contains the CCPA and CPRA required provisions regarding: categories of information collected, purposes of use, retention, etc. This requirement is unrealistic in practice and unmanageable at scale, especially for global businesses that have users around the world. A business would have to collect more information in order to *identify* all California users and link to its CPRA privacy notice for those users, and then ensure that all other users are directed to their regular privacy policy. Alternatively, the business could combine its California privacy notices into its main policy, and then for *every* point of collection of personal information send the user to the specific section that covers their jurisdiction based on the location of the visitor. This requires

businesses to continuously collect or infer the geolocation of all visitors to their website. Either solution is unmanageable at scale.

Additionally, sending individuals to a specific section in the privacy policy deprives users of the full context of the policy, which may help them understand a business's data handling practices and certain global definitions, thus further confusing users. We suggest removing this requirement altogether and allowing businesses to link to their privacy policy. At most, direct links should only be required for situations where it clearly benefits the user to be linked directly to the relevant section.

Determining relevancy is difficult in practice and may not be feasible in all instances. For example, if a company is notifying users of the use of cookies and the company has consolidated information on cookies in one place in their privacy policy, it may make sense for the company to link directly to the cookie section of the privacy policy. However, if the company is notifying the user of the collection of a new data category, it may not make sense to link to a particular section of the privacy policy if the use of the data category is addressed in multiple parts of the privacy policy. Linking to one section would not give users a comprehensive understanding of the use and would be detrimental rather than beneficial.

Proposed section 7012(g) of the draft regulations requires both the first party and the third party to provide a Notice at Collection. Additionally, the first party and third party may be required to provide a single Notice at Collection that includes the required information about their collective Information Practices. This section is almost impossible to apply to complex processing operations that involve different stages of the analysis process, technical activities, and actors involved at different points in the value chain, such as artificial Intelligence or the internet of things. This level of detail is unnecessary, and we suggest removing this section.

## **§ 7026. Requests to Opt-Out of Sale/Sharing**

In proposed section 7026(a)(1), the added limitation for processing in frictionless manner should be removed because the alternatives and the benefits to the consumer are unclear.

We suggest the following change to section 7026(a)(1) (TechNet deletions in ~~strikethrough~~):

"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."

Finally, we appreciate the changes to proposed section 7026(f)(3) and (g), which eliminate requirement to notify third parties about opt-out choices with respect to data shared prior to the opt out and softens the requirement to display opt out status respectively. The change to section 7026(g) will help reduce compliance costs for businesses and confusion for consumers by decluttering the consumer's user experience on certain sites, platforms, or applications by providing the option to display the opt out status.

### **§ 7304. Agency Audits**

Proposed section 7304 would compel businesses to undergo announced or unannounced audits without providing sufficient procedures, processes, or other guidance regarding the scope or nature of these audits. The proposed regulations do not define foundational terms like "audit" or explain how "audits" differ from the law enforcement investigations the Agency is also empowered to conduct.

The proposed regulations should provide additional guidance on the scope of the Agency's "audit" authority and how these audits will be conducted. In developing this guidance, the Agency's oversight role should be exercised in a manner that reflects other important policy considerations, including legitimate businesses' ability to run their operations and receive adequate notice of an audit. Unannounced audits threaten to be non-productive and a poor use of limited Agency resources, because the business will not have time to review requests for material in advance, prepare the requested materials, and identify relevant personnel with information requested. To support the Agency's role in conducting audits to ensure compliance with the law, and to provide businesses with additional guidance and certainty, the regulations also should provide reasonable limitations on the circumstances under which the Agency may conduct audits and the processes by which it does so.

We suggest amending proposed section 7304 to provide businesses with written notice at least 30 days in advance of any audit, including the date of the audit, the matters or areas the Agency intends to audit, and the Agency's basis for auditing the identified matters or areas. We also suggest including a requirement to complete the audit within 180 days from the audit's start date unless otherwise agreed to by the parties.

### **§§ 7301. Agency Initiated Investigations, 7302. Probable Cause Proceedings**

Proposed section 7301 should provide additional guidance and limitations on Agency-initiated investigations. The proposed regulations should provide additional certainty for businesses by clarifying that an investigation can be initiated where the Board, by a majority vote, finds reasonable suspicion that a business has violated the CCPA. This will benefit businesses by ensuring that investigations will not be initiated where there is not a reasonable suspicion that a violation occurred. It will also benefit the Agency by conserving resources to focus on instances where a reasonable suspicion of a violation exists, and reducing the potential for claims that investigations are unfounded or an abuse of authority.

The CPRA allows the Agency to initiate probable cause hearings for alleged violations where the alleged violator is served with a notice that provides a summary of the evidence and the alleged violator is informed of their right to be present. In order to ensure due process, the Agency should require that the notice contain a clear statement of the claims to be addressed at the probable cause hearing, a summary of the evidence in support of each such claim, and the documents and other evidence on which the Enforcement Division Staff will rely at the proceeding. Proposed section 7302 also states that probable cause proceedings "may be conducted in whole or in part by telephone or videoconference," where the proceeding is "not open to the public." While convenience for the parties and cost minimization are worthy goals, the CPRA explicitly grants alleged violators the "right to be present in person" at probable cause proceedings. Thus, the Agency should revise the proposed regulations to clarify that businesses have the right to a live proceeding upon request, even in the case of private proceedings.

The Agency should also confirm that unless the alleged violator requests otherwise, information or arguments presented at the probable cause hearing shall not be shared with the public, as is the case for the notice and probable cause determinations. Additionally, to ensure that businesses receive any probable cause determination made as a result of the proceeding, the proposed regulations should clarify the manner by which probable cause determinations must be delivered and to whom they must be addressed. The regulations should also clarify that the Agency's probable cause determination is only "final" for the purpose of determining that the Agency may hold an administrative hearing to determine whether there has been a violation of the CCPA.

## **Reasonable Implementation and Enforcement Period**

The CPRA goes into effect January 1, 2023. However, this proposed rulemaking has been significantly delayed and is not expected to finalize regulations until the end of January 2023, at the earliest. These regulations contemplate significant new compliance measures for companies and do not even address all of the Agency's statutorily mandated topics for rulemaking. Notably absent, for example, is any meaningful guidance regarding the requirements and technical specifications for



opt-out preference signals. See, section 1798.185(a)(19). Considering the Agency has failed to meet its statutorily required deadline of July 1, 2022 for final regulations it should provide in the proposed regulations, or, at a minimum, voluntarily agree to not undertake enforcement actions with respect to any violations that occur within a 12-month period from the date of the final regulations (as contemplated by Section 1798.185(d)).

While we appreciate that the modified regulations include an optional directive for the Agency to “consider all facts it determines to be relevant, including the amount of time between the effective date of the statutory or regulatory requirement(s) and the possible or alleged violation(s) of those requirements, and good faith efforts to comply with those requirements,” we believe this falls short of providing businesses sufficient time to implement and ensure compliance with the regulations. Businesses deserve greater certainty that they will not be the subject of unfair and burdensome investigations and enforcement actions when they were not provided enough time to review and implement these regulations. If the Agency will not voluntarily agree not to undertake enforcement actions in order to give 12-months for compliance, the regulations should be amended to impose the regulator delay and good faith compliance as a mandatory consideration in the exercise of its enforcement discretion.

## **Conclusion**

We appreciate your consideration of these critically important issues. As privacy laws proliferate throughout the United States, it is even more crucial to enhance the clarity and interoperability of laws and regulations that will allow companies to comply with the requirements set out by various locales. We believe the comments outlined above balance industry operability not only with the CPRA, but with existing omnibus privacy legislation throughout the world. If you need any further information or have any questions about our comments, please contact Dylan Hoffman at [REDACTED]

Sincerely,

[REDACTED]

Dylan Hoffman  
Executive Director, California and the Southwest  
TechNet

---

**From:** Hilary Cain [REDACTED]  
**Sent:** Monday, November 21, 2022 7:23 AM  
**To:** Regulations  
**Subject:** CCPA Public Comment (Alliance for Automotive Innovation)  
**Attachments:** Auto Innovators Comments CCPA Proposed Rules Modifications FINAL 11.21.22.pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good Morning –

Please find attached comments from the Alliance for Automotive Innovation on the modifications to the proposed regulations.

Cheers,  
Hilary

**Hilary M. Cain**  
Vice President - Technology, Innovation, & Mobility Policy  
**O:** [REDACTED]  
**Alliance for Automotive Innovation**  
1050 K Street, NW - Suite 650 Washington, DC 20001  
[REDACTED]





November 21, 2022

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

**RE: Notice of Modifications to Text of Proposed Regulations ([OAL FILE NO. 2022-0628-02](#))**

Dear Mr. Soublet:

The Alliance for Automotive Innovation (“Auto Innovators”) welcomes the opportunity to provide feedback to the California Privacy Protection Agency (“Agency”) on its notice of modifications to the proposed regulations to implement the California Consumer Privacy Act (“CCPA”).

Auto Innovators is the singular, authoritative, and respected voice of the automotive industry. Focused on creating a safe and transformative path for personal mobility, Auto Innovators represents the manufacturers that produce nearly 98 percent of cars and light trucks sold in the United States. In addition to motor vehicle manufacturers, members of Auto Innovators include original equipment suppliers, technology companies, and others within the automotive ecosystem. The auto industry is the nation’s largest manufacturing sector, contributing \$1.1 trillion to the United States economy. As a significant engine for our nation’s economy, the auto sector is responsible for 10.3 million jobs and \$650 billion in paychecks annually.

Our comments below largely reiterate our prior comments to the Agency. These include our written comments in response to the Notice of Proposed Rulemaking, our written comments in response to the Agency’s invitation for preliminary comments on proposed rulemaking, and our oral comments at the pre-rulemaking stakeholder session in May.

While the modifications address some of our concerns, many of the issues that we previously identified that may have inadvertent or unintended impact on the auto industry and its ability to deliver a cleaner, safer, and smarter transportation future remain. We respectfully request an opportunity to meet directly with the Agency to discuss these remaining issues, answer any questions that the Agency may have about their impact on the auto industry, and hopefully work together collaboratively to address them.

### **Effective Date**

We reiterate our request that sufficient lead time be provided between the finalization of this significant rulemaking and the effective date of any new obligations or requirements. As we have previously stated, our member companies take their compliance obligations seriously and need adequate time to align their processes and mechanisms with any new regulatory requirements.

Moreover, we request that any new obligations in the regulations be prospective and apply only to data collected after the regulation's effective date. We previously urged the Agency to reconsider the provision within Section 7014 of the proposed regulations that requires a business to obtain the consent of the consumer before using or disclosing sensitive personal information the business collected "during the time the business did not have a notice of right to limit posted." This appears to create an obligation with respect to data collected before the regulations and the requirement to post a "notice of right to limit" takes effect.

### **Right to Correct**

We urge the Agency to strike the requirement in Section 7023 of the proposed regulations that a business, upon request, disclose all of the specific pieces of personal information that the business maintains and has collected about the consumer to allow the consumer to confirm that the business has corrected the inaccurate information that was the subject of the consumer's request to correct. If the goal is to allow the consumer to confirm that the business has corrected the inaccurate information that was the subject of the consumer's request to correct, it should be sufficient for the business to disclose to the consumer only the specific pieces of personal information that were subject to the consumer's request. At the very least, the Agency should reconsider the provision that specifies that disclosure under this provision is not considered a response to a request to know which is limited to two requests within a 12-month period. If the business is required to disclose all of the specific pieces of personal information that the business maintains and has collected about the consumer, the disclosure should be considered a request to know and be covered by the limitation on two requests within a 12-month period.

### **Consumer Verification for Request to Opt-Out and Request to Limit**

We encourage the Agency to create an exception to the provision in Section 7060 that restricts a business from requiring a consumer to verify the consumer's identity to make a request to opt-out of sale/sharing or to make a request to limit to situations where the sharing or personal information or the use of sensitive personal information is necessary to support a product or service previously requested by the consumer. For example, if the consumer has previously opted into a service through which vehicle data is shared with an insurance company or a service in which geolocation information may be collected following a collision to dispatch emergency responders to the scene of the incident and opting out of sharing or limiting the use of sensitive information would essentially void the ability of the consumer to continue to receive those requested services, it would be entirely appropriate for the business to verify that the consumer is in fact who they claim to be. This would help avoid a situation where someone other than the person who opted into those services could void those services, having a significant negative impact on the person, without that person's knowledge or consent.

### **Contract Requirements for Third Parties**

We reiterate our request that the Agency provide sufficient time (i.e., no less than 6 months) for businesses to develop or renegotiate contracts with third parties with which a business shares or sells a consumer's personal information consistent with such requirements in Section 7053.

### **Agency Audits**

We once again encourage the Agency to remove the ability of the Agency to audit a business "if the subject's collection or processing of personal information presents significant risk to consumer privacy or security" under Section 7304. The Agency should not have the ability to audit a company for this reason alone without any other indication that there has been a possible violation of the CCPA or in the absence of a history of noncompliance with the CCPA or any other privacy protection law.

We also recommend that a reasonable statute of limitations (e.g., three years) be established with respect to the Agency's ability to audit a business. In other words, the Agency's ability to audit compliance should not be limitless and should instead be confined to a specified number of years prior to the initiation of the audit. This approach would be consistent with the model used by other agencies, such as banking and finance agencies, that conduct audits of business.

Consumer privacy remains a priority for the auto industry. We appreciate the opportunity to provide this feedback on the proposed regulations and look forward to an opportunity to discuss these concerns directly with the Agency.

Sincerely,

A solid black rectangular box redacting the signature of Hilary M. Cain.

Hilary M. Cain  
Vice President  
Technology, Innovation and Mobility Policy

---

**From:** Greaves, Fielding [REDACTED]  
**Sent:** Monday, November 21, 2022 7:27 AM  
**To:** Regulations  
**Cc:** Moira Topp; Brousseau, Simonne; Capizzi, Mary Devlin; Kuzma, Clare M.; Andrea Correia; Blenkinsop, Peter; Cher Gonzalez; Stephen Cutie; Sam Chung  
**Subject:** CPPA Public Comment - Life Sciences Coalition Comments 11/21/22  
**Attachments:** CPRA November 3 Proposed Modified Draft Regulations - Life Sciences Coalition Comments 11-21-22.pdf

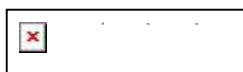
**Importance:** High

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hello,

Please accept the attached comments for the proposed modified draft regulations published November 3, 2022.

Please let me know if you have any questions.



**Fielding Greaves**

Sr. Director, State Government Affairs

San Diego | Los Angeles | Bay Area | **Sacramento** | Washington, D.C. | Tokyo

1111 L Street | Sacramento, CA 95814

[REDACTED] | [www.biocom.org](http://www.biocom.org)





November 21, 2022

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

Via email to [regulations@cpha.ca.gov](mailto:regulations@cpha.ca.gov)

**Subject: Public Comment on Notice of Modifications to Text of Proposed Regulations  
 (Nov. 3, 2022)**

Dear California Privacy Protection Agency:

Biocom California<sup>1</sup>, California Life Sciences (“CLS”)<sup>2</sup>, and the International Pharmaceutical & Medical Device Privacy Consortium (“IPMPC”) welcome the opportunity to provide comments on the Agency’s modifications to the proposed regulations implementing the Consumer Privacy Rights Act of 2020 (“CPRA”) and revising the regulations issued previously under the California Consumer Privacy Act of 2018 (“CCPA”).<sup>3</sup>

The IPMPC is comprised of chief privacy officers and other data privacy and security professionals from a number of research-based, global pharmaceutical and medical-device manufacturers. The IPMPC is the leading voice in the global pharmaceutical and medical device industry to advance innovative privacy solutions to protect patients, enhance healthcare, and support business enablement.<sup>4</sup>

We thank the Agency for considering the comments we submitted on the text of the proposed regulations published on July 8, 2022, and we have taken note of those modifications to the proposed regulations that address some of our prior comments. We also continue to encourage the Agency to add further examples to illustrate key concepts. With the sunset on January 1, 2023 of the exemptions contained in Civil Code §§ 1798.145(m) and (n), it would be particularly helpful to add practical, real-world illustrations showing how the proposed regulations apply to personal information concerning employees, job applicants, and independent contractors to a business, as well as to business-to-business contacts. Moreover, we ask that the Agency delay the effective date of the revised regulations to provide at least six months for businesses to implement necessary compliance measures.

Additional comments on specific provisions follow below:

**§ 7025(e). Opt-Out Preference Signals, processing choices.**

<sup>1</sup> More information about Biocom California is available at <https://www.biocom.org>.

<sup>2</sup> More information about CLS is available at <https://www.califesciences.org>.

<sup>3</sup> These comments reflect the positions of Biocom California, CLS, and IPMPC as organizations and should not be necessarily construed as the positions of any individual member.

<sup>4</sup> More information about the IPMPC is available at <https://www.ipmpc.org>.

We have previously commented that the Agency’s statement that 1798.135(b) “does not give the business a choice between posting the above-referenced links or honoring opt-out preference signals” conflicts with the plain language of 1798.135(b) and (c). 1798.135 sets up two approaches for facilitating opt-out requests – a business can choose to either post the links or to honor consumer opt-out “signals.” Doing both is expressly not required. 1798.135(b)(3) makes it very clear that “a business may elect whether to comply with subdivision (a) [posting links] or (b) [honoring opt-out signals].”

The Agency’s proposed approach requires businesses to allow consumers to opt-out via a preference signal, and the Agency states that the only choice a business is allowed is whether to process opt-out signals on a “frictionless” or “non-frictionless” basis. However, neither of these terms appear in the CPRA. The CPRA does not contemplate two different kinds of responses to opt-out signals – it just describes two options for receiving such signals.

**§ 7051(e). Contract Requirements for Service Providers and Contractors. Contractual due diligence.**

Section 1798.145(i)(1) states that “[a] business that discloses personal information to a service provider or contractor in compliance with this title shall not be liable under this title if the service provider or contractor receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider or contractor intends to commit such a violation.” This section thereby establishes a misconduct or gross negligence standard for a business’s loss of liability protection. However, in the proposed regulations, the Agency states that “[w]hether a business conducts due diligence of its service providers and contractors factors into whether the business has reason to believe that a service provider or contractor is using personal information in violation of the CCPA and these regulations.” The Agency further states that a business that “never enforces the terms of the contract nor exercises its rights to audit” a service provider may not claim it did not know and should not have known of a service provider’s violation. The Agency’s proposed approach follows a mere “negligence” standard for loss of liability protection. This conflicts with the express language of Section 1798.145(i)(1).

**Conclusion and contact information.**

Thank you for considering our comments and recommendations. If you have any questions, you may contact Fielding Greaves at [REDACTED] Sam Chung at [REDACTED] or Peter Blenkinsop at [REDACTED].

Sincerely,

[REDACTED]

Fielding Greaves  
Sr. Director, State Government  
Affairs  
Biocom California

[REDACTED]

Sam Chung  
Vice President, State  
Government Relations  
California Life Sciences (CLS)

[REDACTED]

Reed Abrahamson  
Secretariat  
International Pharmaceutical &  
Medical Device Privacy  
Consortium (IPMPC)



---

**From:** Matthew Schwartz [REDACTED]  
**Sent:** Monday, November 21, 2022 7:33 AM  
**To:** Regulations  
**Subject:** CPPA Public Comment - ACT | The App Association  
**Attachments:** ACT - The App Association Comments on Proposed Modifications to Rulemaking under the California Privacy Rights Act of 2020.pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good morning,

Attached please find comments of ACT | The App Association in response to the CPPA's proposed modifications to the rules under CPRA.

Best,

Matt Schwartz  
*Policy Associate*  
**ACT | The App Association**

P [REDACTED]  
E: [REDACTED]



November 21, 2022

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

**RE: ACT | The App Association Comments on Proposed Modifications to Rulemaking under the California Privacy Rights Act of 2020**

**I. Introduction and Statement of Interest**

ACT | The App Association (App Association) appreciates the opportunity to submit comments in response to the California Privacy Protection Agency’s (CPPA or Agency) call for input regarding its draft modifications of its proposed rules under the California Privacy Rights Act of 2020 (CPRA). The App Association appreciates that many of the Agency’s proposed modifications in this round of rulemaking improve clarity for small businesses, like our member companies, as well as for consumers. At the same time, we continue to believe many of the regulations need further refinement, especially in light of the rapidly approaching enforcement date.

The App Association represents thousands of small business software application development companies and technology firms, including many based in California and/or conducting business in California and falling within the scope of law. Our member companies create technologies that generate internet of things (IoT) use cases across consumer and enterprise contexts and are primary drivers of the global digital economy. Today the ecosystem the App Association represents—which we call the app economy—is valued at approximately \$1.7 trillion and is responsible for tens of millions of jobs around the world, including 702,010 in California alone.<sup>1</sup> The growth of this vital ecosystem is expected to continue; worldwide consumer spending in mobile apps is projected to reach \$171 billion by 2024, more than double the \$85 billion from 2019.<sup>2</sup>

Consumers who rely on our members’ products and services expect that our members will keep their valuable data safe and secure. Our members practice responsible and efficient data usage to solve problems identified across consumer and enterprise use cases. Their customers have strong data security and privacy expectations and, as such, ensuring that the company’s business practices reflect those expectations by utilizing the most advanced technical protection mechanisms (e.g., end-to-end encryption) is a market-driven necessity.

<sup>1</sup>See *State of the U.S. App Economy: 2020*, ACT | THE APP ASSOCIATION, (2020) available at: <https://actonline.org/wp-content/uploads/2020-App-economy-Report.pdf> (noting that California has an estimated 702,010 app economy workers as of 2020).

<sup>2</sup> Sarah Perez, *Mobile app spending to double by 2024, despite economic impacts of COVID-19*, TechCrunch (Apr. 1, 2020), <https://techcrunch.com/2020/04/01/mobile-app-spending-to-double-by-2024-despite-economic-impactsof-covid-19/>

The App Association serves as a leading resource in the privacy space for thought leadership and education for the global small business technology developer community.<sup>3</sup> We regularly work to keep our members up to speed on the latest policy and legal developments and to translate those into practical and useable guidance, including on California privacy law, to ease the burden of compliance.<sup>4</sup>

## II. General Comments

In general, we appreciate the effort the Agency clearly poured into streamlining many of the regulations and improving overall readability. We also thank the Agency for acting with haste to put into practice the suggestion of board member Vinhcent Le, made at the October 29 Agency board meeting, to require that the Agency take into account the timing of final regulations when considering enforcement actions. The amended Section 7301 (b) permits that the Agency “may” consider the amount of time between the effective date of the regulatory requirements and the possible or alleged violation(s) of those requirements, as well as good faith efforts to comply with those requirements.<sup>5</sup>

The Agency signaling that it recognizes that businesses are working with expedited timelines to incorporate the final revisions to the rules into their compliance programs is an important step in reducing enforcement-related anxiety. However, we remain concerned that the finalization of these rules (which are just a subset of the full slate of rules to be issued by the Agency) is likely to occur after the effective date of the law. Strengthening the operative instruction in Section 7301 (b) from “may” to “shall” so that the Agency is *required* to take into account the proximity of the final rules to any alleged violation, at the very least for sections of the rules that have been substantially rewritten in this latest round of rulemaking, would eliminate any remaining fear that businesses could be penalized for failing to comply with rules not even finalized at the time of the law’s effective date.

## III. Comments on Specific Topics Addressed in the Draft Regulations

### *Definitions*

In the previous round of comments, we suggested that the term “disproportionate effort” in the context of responding to consumer requests should be inclusive of cases when retrieving the requested information introduces a cybersecurity risk due to the age and/or location of the requested data (for example, data that only exists on archived drives). The new

---

<sup>3</sup> See e.g., ACT | The App Association, *Innovators Network Foundation Announces Inaugural Privacy Fellows* (September 2019), available at: <https://actonline.org/2019/09/23/innovators-network-foundation-announces-inaugural-privacy-fellows/>.

<sup>4</sup> See e.g., ACT | The App Association, *General Data Protection Regulation Guide* (May 2018), available at: [https://actonline.org/wp-content/uploads/ACT\\_GDPR-Guide\\_interactive.pdf](https://actonline.org/wp-content/uploads/ACT_GDPR-Guide_interactive.pdf); *What is the California Consumer Privacy Act (January 2020)*, available at: <https://actonline.org/wp-content/uploads/What-is-CCPA.pdf>.

<sup>5</sup> CCPA Proposed Regulations, §7031 (b)

modifications potentially resolve this by allowing businesses to weigh “the technical limitations impacting their ability to respond” when determining if the time and resources they would need to leverage in order to respond outweighs the “reasonably foreseeable material impact” to the consumer by not responding.<sup>6</sup> One addition to strengthen this section and clarify that it includes cybersecurity considerations would be to add the term “or technical risks” after “technical limitations.” While it may be *technically* possible for some businesses to respond to consumer requests by accessing archived data drives, it may introduce unacceptable levels of risk that outweigh the reasonably foreseeable harm to consumers from not responding.

Reiterating our comment from the last round, we also suggest that the regulations consider a more granularized framework for the treatment of individual requests in light of the inclusion of household-level data in the definition of “personal information.” Previous Subsection K, defining “household” has been removed from the regulations, as the term is now defined through the text of CPRA.<sup>7</sup> However, since CPRA states that personal information includes information that can be reasonably linked to a household, individuals within a household are at risk for having their opt-out preferences or consumer requests dictated by other members of their household. For example, many apps currently allow multiple users on the same device or account to create individualized preferences through user profiles. If one user of that device decides to opt out or requests that the business delete their data, it is unclear how the business can honor the requests of a different user of that same device that selects a different set of preferences.

### *Restrictions on the Collection and Use of Personal Information*


In the previous round of comments, we noted that the concepts of “explicit consent” and “average consumer” used in Section 7002 were unnecessarily ambiguous, and we appreciate that the proposed modifications remove references to both concepts. In the place of the concept of the “average consumer,” the regulations now state that businesses may only collect or process personal information in line with the “reasonable expectations” of the consumer, a test based on five factors. This markedly improves clarity and gives businesses a more tangible measuring stick by which to evaluate whether their collection or use of personal information is compatible, especially when compared to evaluating the expectations of the nebulous “average consumer.” At the same time, we believe the second factor, “[t]he type, nature, and amount of personal information that the business seeks to collect or process,”<sup>8</sup> should be broadened to include the use of personal information to improve the service for which the data was collected.

We do not believe that it is an unexpected use of data to improve the service for which the consumer consented, unlike, for example, the collection of geolocation data to run a flashlight application. The example the Agency provides this time around, a business that collects the

<sup>6</sup> CPPA Proposed Regulations, §7001 (i)

<sup>7</sup> California Civil Code § 1798.140 (q)

<sup>8</sup> CPPA Proposed Regulations, §7002 (b)(2)



consumer's fingerprint in connection with setting up a security feature that unlocks the device using the fingerprint, is illustrative. As written, this example could be viewed to preclude *improvements* to the service, since the Agency writes that the “consumer likely expects that the business’s use of the consumer’s fingerprint is *only* for the purpose of unlocking their mobile device” [emphasis added].<sup>9</sup> In reality, the consumer likely also has expectations that the business uses that information to continually improve the service in order to keep their device secure, for example when new research regarding the efficacy of fingerprint identification comes to light.

In the place of “explicit consent,” the Agency now simply writes that the business shall obtain the consumer’s “consent” in accordance with Section 7004.<sup>10</sup> As previously noted, the text of CPRA already clarifies the meaning of consent, and based on a plain reading, it seems consent requires an affirmative and informed decision by the consumer, which ostensibly also meets the definition of explicit. We thank the Agency for adopting this change.

### *Privacy Policies*

The App Association is concerned that the requirements remain universal for businesses to provide detailed information in their privacy policies about to how they will process user opt out preference signals, including information about “whether the signal applies to the device, browser, consumer, account, and/or offline sales, and in what circumstances” and whether they process opt-out preference signals in a “frictionless manner.”<sup>11</sup>

While the presence of such requirements make sense in light of CPRA's language referencing the ability for businesses to honor user opt-out preference signals, many smaller businesses may not even know about the existence of user opt-out preference signals, let alone that they must post detailed information about the way they intend to process them. This requirement may especially come as a surprise for businesses that do not sell or share personal information, considering the opt-out preference signal only currently communicates the consumer choice to opt out of the sale and sharing of personal information. Seeing as how there is likely little value to consumers in receiving information about how businesses intend to operationalize a technology that has no effect on the businesses’ activities, we reiterate that this requirement should be optional for businesses that do not sell or share personal information but nonetheless meet the coverage threshold for the law.

### *Notice at Collection*


We thank the Agency for amending Section 7012 (g)(2) to read that a third party that controls the collection of personal information on the first party's *physical premises* must only provide a notice at collection at the physical premise. Without this clarification, the section could have been interpreted to require third parties to provide notice of collection at the physical location

---

<sup>9</sup> Ibid.

<sup>10</sup> CPPA Proposed Regulations, §7002 (e)

<sup>11</sup> CPPA Proposed Regulations, §7011 (3)(F-G)



of any first party for which they control collection, even if that collection occurs online, which would have resulted in third parties issuing unduly confusing and duplicative notices.

### *Obtaining Consumer Consent*

We continue to urge the Agency to provide examples of language that is "easy to understand," in the context of businesses designing CCPA request processes and obtaining consumer consent (Section 7004). While the rule directs businesses to Section 7003 for further guidance, that Section simply states that language should be "plain, straightforward language and avoid technical or legal jargon."<sup>12</sup> It may help businesses for the Agency to provide several examples of what it considers overly complex or difficult to understand language. Given that the rights granted through CCPA and now CPRA are still relatively new to consumers and somewhat inherently complicated (e.g., documentation for requests to correct) due to the nature of the statute and rules, crafting exceptionally simple language here may be difficult.

In lieu of that, we again urge the Agency to consider a more objective standard than "easy to understand" considering the ranges of age and sophistication of consumers submitting requests. Given the relative complexity of the underlying information businesses communicate with such notices, a high school graduate reading level might be the appropriate standard to index against.

### *Universal Opt Out*


While we continue to question the Agency's authority to require the recognition of consumer opt-out preference signals, we appreciate the amendments in Section 7025 (b) to recognize that businesses covered by CPRA that do not sell or share personal information should not be required to process consumer opt-out preference signals. We also appreciate that Section 7025 (c) (6) has been amended to so that businesses "may" display whether they have processed consumer opt-out preference signals. Such a confirmation requirement would have unnecessarily required businesses to devote engineering resources to build a confirmation tool that would have served no tangible benefit to consumers.

### *Methods for Submitting Requests to Delete, Requests to Correct, and Requests to Know*

We continue to urge the Agency to affirm that businesses that follow the requirements in Section 7020 to correct personal information are using the "commercially reasonable practices" required by CPRA. As noted previously, CPRA does not attach a similar "commercially reasonable" requirement to requests to delete or know, which are also addressed Section 7020.

---

<sup>12</sup> CCPA Proposed Regulations, §7002 (a)



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

CPRA expands the 12-month disclosure period for a consumer's right to know. Consumers may request to know about any new personal information collected or processed on or after January 1, 2022, even if that information is more than 12 months old at the time of the request, subject to certain exceptions detailed in the regulation. The App Association urges the CPPA to adopt a common-sense exception inclusive of instances where the business (1) migrated its data prior to the 12-month lookback to new storage facilities or service providers, (2) otherwise does not maintain access to the requested data, or (3) cannot make the requested data accessible without creating a significant cybersecurity risk.

*Requests to Limit Use and Disclosure of Sensitive Personal Information*

We continue to take issue with Section 7060, which currently prohibits businesses from requiring that a consumer verify their identity before making a request to opt out of sale or sharing or making a request to limit the use of sensitive information.<sup>13</sup> The Initial Statement of Reasons justifies this decision by saying that "the potential harm to consumers from non-verified requests is minimal."<sup>14</sup>

We disagree, as in the case of limiting the use of sensitive information, the damage of a fraudulent request can be significant. Since requests to limit sensitive information reduce permitted data uses to those "reasonably expected by an average consumer,"<sup>15</sup> disruptions to a person's requested services could be significant depending on how broadly that provision is interpreted (for example, if improvements to the service are not considered to be reasonably expected). For example, in the connected healthcare context, improvements to a person's diagnostics could be seriously altered by a fraudulent request to limit sensitive data without them even realizing a change has been made. We urge the Agency to allow for verification of requests to limit sensitive information and, in general, caution the Agency against taking the stance that a person's decision to share sensitive information was made trivially and should be able to be easily undone.

While we recognize that the amendments to Section 7027 will reduce the total amount of sensitive personal information subject to requests to limit since it exempts from requests to limit any "sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer," the information *most* vulnerable to unverified requests to limit remains untouched.<sup>16</sup>

---

<sup>13</sup> CPPA Proposed Regulations, §7060 (b)

<sup>14</sup> CPPA Initial Statement of Reasons § 7060 (b)

<sup>15</sup> CPPA Proposed Regulations, §7027 (m) (1)

<sup>16</sup>CPPA Proposed Regulations, 7027 (m)(8)

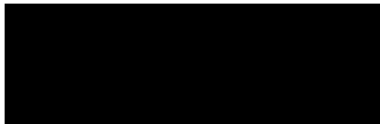


#### IV. Conclusion

The App Association strongly supports privacy regulation that upholds the mission of consumer protection and sets a clear baseline set of expectations for the businesses that are required to comply. From the small business perspective, it is also vital that privacy regulations create a predictable and consistent legal landscape and is scalable such that smaller entities can continue to comply and compete with larger entities. We are hopeful that the CCPA can strike the appropriate balance in future rulemaking activities.


We thank the CCPA in advance for its consideration of our views, and we look forward to engaging further in the future.

Sincerely,



Brian Scarpelli  
Senior Global Policy Counsel

Matt Schwartz  
Policy Associate

ACT | The App Association  
1401 K St NW (Ste 501)  
Washington, DC 20005  
e: 



---

**From:** Colby Williams [REDACTED]  
**Sent:** Monday, November 21, 2022 7:32 AM  
**To:** Regulations  
**Subject:** SIA Public Comment Re: CCPA Regulations  
**Attachments:** SIA Public Comment\_CPPA\_11.21.2022.pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

To whom it may concern,

Please see the attached for the Security Industry Association's (SIA) public comment on the California Privacy Protection Agency's latest modifications made to the regulations proposed implementing the California Consumer Privacy Act.

Please confirm receipt of our public comment.

Thank you,

**Colby Williams**  
Senior Manager, Government Relations  
Security Industry Association (SIA)  
[REDACTED]

Confidentiality Note: This message and any attachments may contain legally privileged and/or confidential information. Any unauthorized disclosure, use or dissemination of this e-mail message or its contents, either in whole or in part, is prohibited. The contents of this email are for the intended recipient and are not meant to be relied upon by anyone else. If you are not the intended recipient of this e-mail message, kindly notify the sender and then destroy it.



November 21, 2022

California Privacy Protection Agency (CPPA)  
Attention: Brian Soublet  
2101 Arena Blvd.  
Sacramento, CA 95834

To Whom It May Concern:

**Re: Notice of Proposed Rulemaking, California Privacy Protection Agency (November 3, 2022)**

The Security Industry Association (SIA) appreciates the opportunity to submit public comment on the Modified Proposed Rules to amend California's privacy regulations to implement the California Consumer Privacy Act (CCPA).

SIA Represents nearly 200 companies headquartered in California that provide a wide array of products essential to protecting the physical safety of people property, businesses, schools, and critical infrastructure in the state and throughout the nation. This includes access control, alarm systems, security camera systems, screening and detection equipment, and many other applications. Our member companies are deeply committed to safeguarding personal information through their own business practices as well as the design of the products and services they provide that collect and process information.

It is critical that the California Consumer Privacy Act Regulations ensure the continued functionality and effectiveness of safety and security technology applications. However, we are concerned that if unaddressed in the final regulations, the latest draft language of the proposed modifications will create ambiguities that could impede the functionality and reduce the benefits to businesses and consumers of security systems, as well as hamper investigations.

**Specifically, clarification is needed to address incongruity between sections 7002 and 7027(m) concerning use of information for security purposes.** Significant new language added to Sec. 7002 (Restrictions on the Collection and Use of Personal Information) could be interpreted to require that the collection and processing of personal information by businesses must *either* follow the provision of consumer consent *or* it must be for purposes consistent with the reasonable expectations of the consumers (or in a compatible context) as defined in Sec. 7002 (b) and (c), without additional contextual considerations. These restrictions appear to be incongruous with the exceptions in Sec. 7027(m), which expressly recognize the importance of certain security-related processing activities.

Given the need for broad data collection and the inability at times to notify a consumer in advance of security monitoring and investigations (such as using security camera recordings), obtaining the consent of each and every person who is subject to security monitoring or investigations is not only impracticable, but it also runs counter to the purpose of the use of the technology.

Sec. 7002 could therefore be perceived to prohibit the collection and processing of any personal information for security purposes if it is not sufficiently consistent with a consumer's reasonable expectations. However, all the example scenarios in Sec. 7002(b) for determining consistency with a consumer's reasonable expectations are provided in the context of online data collection from consumers via websites or apps. This does not clearly translate to the collection of personal information where there is a physical context, where data is often collected for security purposes from other sources or from indirect observation.

Given these factors laid out in Sec. 7002(b) in the latest draft, there is significant ambiguity as to whether a business can use data for a security purpose where such data is commonly collected 1) originally for a non-security purpose, (2) from a source other than the consumer, or (3) from general observations of the consumer.

At the same time, Sec. 7027(m) provides a list of narrowly tailored exceptions to a consumer's right to limit the use and disclosure of their "sensitive personal information." The exceptions expressly recognize the need for flexibility in the security context by not requiring a business to offer a right to limit if the information is used to "resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions" in Sec. 7027(m)(3), or to "ensure the physical safety of natural persons" in Sec. 7027(m)(4).

While Sec. 7002(b)(4) suggests a business may be able to comply with Sec. 7002 by providing all consumers an appropriate disclosure of the use of its security system, it is not clear what level of disclosure would be sufficient. Further, even if these disclosure requirements were sufficiently met by a business, it is unclear whether the other factors set forth in Sec. 7002(b) could outweigh the disclosure, making it difficult for the business to determine whether its security system presents a risk of violating the CCPA.


To address this risk, the CPPA should clarify that these same unique circumstances, under which processing of "sensitive personal information" may not be limited by request, should satisfy the requirements under Sec. 7002(b). This would not only provide greater consistency within the regulations, but it would also avoid unnecessary confusion with potential real-world impact to safety and security.

Given the apparent incongruity between Secs. 7002 and 7027(m), and the important public policy of empowering businesses to protect their employees, patrons, and property, ***the CPPA should modify Sec. 7002 to add clarification that personal information collected and used for the security and investigative purposes in Sec. 7027(m)(3) & (4), would be considered "consistent with the reasonable expectations of the consumer(s) whose personal information is collected or processed."***

The Security Industry Association (SIA) stands ready to work with the CPPA to ensure effective regulations protecting data privacy, which are consistent with statutory authority and promote uniformity, consistency functionality, and clarity in implementation. Please let us know if you have any questions or if we can provide any additional information that would be helpful.

Respectfully Submitted,

  
Don Erickson  
Chief Executive Officer  
Security Industry Association  
Silver Spring, MD  
[www.securityindustry.org](http://www.securityindustry.org)

Staff Contact: Colby Williams, 

---

**From:** Goldrosen, Juliana [REDACTED]  
**Sent:** Monday, November 21, 2022 7:41 AM  
**To:** Regulations  
**Subject:** CCPA Public Comment - County of Santa Clara  
**Attachments:** CCPA Modified Proposed Regulations - Technical Comment 11-21-22.pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

To whom it may concern:

Please see attached for a technical comment from the Office of the County Counsel, County of Santa Clara.

Sincerely,

Juliana Goldrosen



**Juliana Goldrosen** | Deputy County Counsel  
Office of the County Counsel, County of Santa Clara  
70 West Hedding Street, East Wing, 9<sup>th</sup> Floor | San José, CA 95110  
Office: [REDACTED] | Mobile: [REDACTED]  
Pronouns: she/her/hers  
[REDACTED] | [counsel.sccgov.org](http://counsel.sccgov.org)

**NOTICE TO RECIPIENT:** The information in this email is confidential and may be protected by the attorney-client and/or work product privileges. If you received this email in error, any review, use, dissemination, distribution, or copying of it is strictly prohibited. Please notify Administration, Office of the County Counsel, of the error immediately at [REDACTED] and delete this communication and any attached documents from your system.

**OFFICE OF THE COUNTY COUNSEL  
COUNTY OF SANTA CLARA**

County Government Center  
70 West Hedding Street  
East Wing, 9<sup>th</sup> Floor  
San José, California 95110-1770



**James R. Williams  
COUNTY COUNSEL**

Robert M. Coelho  
Michaela L. Lewis  
Tony LoPresti  
Steve Mitra  
Kavita Narayan  
Douglas M. Press  
Gita C. Suraj  
**ASSISTANT COUNTY COUNSEL**

Kim Forrester  
**LEGAL AND COMPLIANCE OFFICER**

November 21, 2022

**VIA EMAIL**

Brian Soublet  
California Privacy Protection Agency  
2101 Arena Blvd.  
Sacramento, California 95834  
[regulations@cpha.ca.gov](mailto:regulations@cpha.ca.gov)

Re: Comment of the Office of the County Counsel, County of Santa Clara on the California Privacy Protection Agency's Modified Proposed Regulations Implementing the California Consumer Privacy Act (OAL FILE NO. 2022-0628-02)

Dear Mr. Soublet:

I write on behalf of the Office of the County Counsel, County of Santa Clara to provide a technical comment on the California Privacy Protection Agency's Modified Proposed Regulations dated November 3, 2022, implementing the California Consumer Privacy Act (CCPA). Protecting and safeguarding individuals' personal information is a vital part of the County's duties. The County has robust privacy and data security protections for all personal information gathered by the County and is one of the few counties in the country to have a dedicated Chief Privacy Officer. The County looks forward to the continued implementation of the CCPA and the revised regulations. The Office of the County Counsel recommends a technical edit to the regulation to clarify the scope of the CCPA's requirements for entities that provide services to "nonbusinesses," including government entities.

The CCPA and these regulations impose different obligations on "businesses" than on "service providers" or "contractors," particularly with regards to requirements for responding to consumers' requests under the CCPA. The CCPA's definition of "business" includes only certain for-profit entities that collect consumers' personal information.<sup>1</sup> The definition of

<sup>1</sup> Cal. Civ. Code § 1798.140(d).

Letter to Brian Soublet, California Privacy Protection Agency  
 Comment of the Office of the County Counsel, County of Santa Clara on the California Privacy Protection Agency's Modified Proposed Regulations Implementing the California Consumer Privacy Act

November 21, 2022

Page 2 of 4

“service provider,” in turn, includes for-profit entities that “process[] personal information on behalf of a *business*” in certain circumstances.<sup>2</sup> Thus, for example, under modified proposed Section 7050(d), a “service provider or contractor” that is also a “business” “shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells *outside* of its role as a service provider or contractor.”<sup>3</sup> Said differently, a “service provider” that is also a “business” need only comply with the CCPA and the regulations with regard to information it collects, maintains, or sells in its role as a “business,” and not with regard to information from another entity that it has access to and processes in its role as a “service provider.”

In its modified proposed regulations, the California Privacy Protection Agency seeks to clarify the obligations on businesses that provide services to non-profits or government entities, since they do not qualify as “service providers” under the CCPA. The modified proposed Section 7050(g) states: “Whether an entity that provides services to a Nonbusiness<sup>4</sup> must comply with a consumer’s CCPA request depends upon whether the entity is a ‘business,’ as defined by Civil Code section 1798.140, subdivision (d).”

However, modified proposed Section 7050(g) would create an inconsistency. This section could be interpreted as requiring a “business” that provides services to a “Nonbusiness” as having to comply with a CCPA request with regard to even the information from a “Nonbusiness” that it processes pursuant to its service to the “Nonbusiness.” In contrast, as stated above, under Section 7050(d) of the modified proposed regulations, a “business” that for some of its activities acts as a “service provider” or contractor to another “business” only has to comply with the CCPA requirements that apply to “businesses” “with regard to any personal information that it collects, maintains, or sells *outside* of its role as a service provider or contractor.”<sup>5</sup>

---

<sup>2</sup> *Id.* at § 1798.140(ag) (emphasis added).

<sup>3</sup> (Emphasis added.) Currently, California Code of Regulations title 11, section 7051(f) states: “A service provider that is a business shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells outside of its role as a service provider.” The modified proposed regulations would make it the new Section 7050(d) and expand the existing provision to include contractors.

<sup>4</sup> Modified proposed section 7001(p) would define “Nonbusiness” as: “a person or entity that does not meet the definition of a ‘business’ as defined in Civil Code section 1798.140, subdivision (d). For example, non-profits and government entities are Nonbusinesses because ‘business’ is defined, among other things, to include only entities ‘organized or operated for the profit or financial benefit of its shareholders or other owners.’”

<sup>5</sup> *Supra* fn. 3.

Letter to Brian Souble, California Privacy Protection Agency  
 Comment of the Office of the County Counsel, County of Santa Clara on the California Privacy  
 Protection Agency's Modified Proposed Regulations Implementing the California Consumer  
 Privacy Act

November 21, 2022

Page 3 of 4

Furthermore, the language of modified proposed Section 7050(g) seems to go against the Agency's stated concerns. The Agency's Initial Statement of Reasons states that, without further clarification through the regulations, "entities that process personal information on behalf of non-profit and government entities in accordance with a written contract may be required to comply with consumer requests even when those non-profits and government entities in ultimate control of the information are not required to do so."<sup>6</sup> As the Agency stated, "[t]his unintended and undesired consequence will lead to significant disruption in the functioning of those non-profits and governmental entities and is not in furtherance of the purposes of the CCPA."<sup>7</sup>

Given these reasons, the Office recommends the following clarifications to modified proposed Section 7050(g) (proposed deletions have a strikethrough and proposed additions are underlined):

If ~~Whether~~ an entity that provides services to any Nonbusiness must comply with a consumer's CCPA request depends upon whether the entity is a "business," as defined by Civil Code section 1798.140, subdivision (d), then it shall comply with a consumer's CCPA request only with regard to any personal information that it collects, maintains, or sells outside of its service to any Nonbusiness.

These clarifications are consistent with the Agency's intentions and the CCPA's treatment of service providers that are also "businesses," and would provide additional guidance to for-profit entities that perform services for nonbusinesses, including government entities.

Thank you for your close attention to this important clarification. We are available to answer any questions or provide any additional information that would be helpful, and we look forward to the final regulations taking this important clarification into account.

Very truly yours,

JAMES R. WILLIAMS  
 County Counsel

---

<sup>6</sup> California Privacy Protection Agency, Initial Statement of Reasons, [https://cppa.ca.gov/regulations/pdf/20220708\\_isr.pdf](https://cppa.ca.gov/regulations/pdf/20220708_isr.pdf).

<sup>7</sup> *Id.*

Letter to Brian Souble, California Privacy Protection Agency  
Comment of the Office of the County Counsel, County of Santa Clara on the California Privacy  
Protection Agency's Modified Proposed Regulations Implementing the California Consumer  
Privacy Act

November 21, 2022

Page 4 of 4

*/s/ Juliana Goldrosen*  
JULIANA GOLDROSEN  
Deputy County Counsel



---

**From:** Emory Roane [REDACTED]  
**Sent:** Monday, November 21, 2022 7:49 AM  
**To:** Regulations  
**Subject:** CCPA Public Comment  
**Attachments:** 2022.11.21 - CCPA Comments - California Privacy Coalition.pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Regards,

Attached are comments sent in response to the CCPA rulemaking period that opened on Thursday, November 3, 2022, and closes at 8:00 am on Monday, November 21, 2022. These comments reflect positions held by:

- The Electronic Frontier Foundation
- ACLU California Action
- Privacy Rights Clearinghouse
- Oakland Privacy
- Media Alliance, and
- The Consumer Federation of America

Sincerely,

Emory Roane  
Policy Counsel  
Privacy Rights Clearinghouse  
3033 5<sup>th</sup> Avenue, Suite 223  
San Diego, CA 92103  
[privacyrights.org](https://www.privacyrights.org)  
[REDACTED]



Privacy Rights  
Clearinghouse



**MEDIA  
ALLIANCE**



OAKLAND  
PRIVACY



Consumer Federation of America

COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION, ACLU CALIFORNIA ACTION, PRIVACY RIGHTS CLEARINGHOUSE, OAKLAND PRIVACY, CONSUMER FEDERATION OF AMERICA, AND MEDIA ALLIANCE

to the

CALIFORNIA PRIVACY PROTECTION AGENCY  
On Proposed Rulemaking Under the California Privacy Rights Act of 2020  
(Comments on Modified Text of Proposed Regulations)

November 21, 2022

### **Introduction**

Our groups are writing in reply to the invitation issued by the California Privacy Protection Agency (“the Agency”) seeking input from stakeholders in developing regulations as directed by the California Privacy Rights Act (CPRA), and the California Privacy Protection Act (CCPA) as modified by the CPRA. These comments are in response to the version of rules that the agency published Nov. 8, 2022.

### **About The Parties**

The **Electronic Frontier Foundation** (EFF) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. With over 35,000 dues-paying members (with several thousand California members) and well over 1 million followers on social networks, we focus on promoting policies that benefit both creators and users of technology. EFF has engaged in discussions around privacy regulations in California and throughout the country at the state and federal level. EFF has previously submitted comments to the California Attorney General regarding rulemaking for the California Consumer Privacy Act (CCPA), both as an individual organization and in collaboration with other leading privacy advocacy organizations.

**ACLU California Action** protects civil liberties and civil rights, advances equity, justice, and freedom, and dismantles systems rooted in oppression and discrimination. ACLU California Action has an abiding interest in the promotion of the guarantees of individual rights embodied in the federal and state constitutions, including the right to privacy guaranteed by the California Constitution and the right to due process. ACLU California Action is a 501(c)(4) organization associated with the three ACLU affiliates in California—

Group Comments

Comments on Modified Text of Proposed Regulations

Page 3 of 14

ACLU of Northern California, ACLU of Southern California, and ACLU of San Diego and Imperial Counties.

**Privacy Rights Clearinghouse** is focused on increasing access to information, policy discussions and meaningful rights so that the right to data privacy can be a reality for everyone. Founded in 1992 to help people understand their rights and choices, it is one of the first and only organizations to focus exclusively on data privacy rights and issues. For three decades, our team has been driven by the beliefs that data privacy is a fundamental human right and essential for an equitable future, and that everyone deserves the opportunity to be informed and be heard.

**Oakland Privacy** is a citizen's coalition that works regionally to defend the right to privacy, enhance public transparency, and increase oversight of law enforcement, particularly regarding the use of surveillance techniques and equipment. As experts on municipal privacy reform, they have written use policies and impact reports for a variety of surveillance technologies, conducted research and investigations, and developed frameworks for the implementation of equipment with respect for civil rights, privacy protections and community control.

**Media Alliance** is a Bay Area democratic communications advocate. Our members include professional and citizen journalists and community-based media and communications professionals who work with the media. Our members are concerned with communications rights, especially at the intersections of class, race and marginalized communities.

**The Consumer Federation of America (CFA)** is an association of non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education. Today, more than 250 of these groups participate in the federation and govern it through their representatives on the organization's Board of Directors. CFA is a research, advocacy, education, and service organization. As an advocacy

Group Comments

Comments on Modified Text of Proposed Regulations

Page 4 of 14

organization, CFA works to advance pro-consumer policies on a variety of issues before Congress, the White House, federal and state regulatory agencies, state legislatures, and the courts. We communicate and work with public officials to promote beneficial policies, oppose harmful ones, and ensure a balance debate on issues important to consumers.

### **Reiterating Concerns about "Financial Incentives" in §7016**

In our previous comments we made several recommendations to ensure that consumers had strong rights. In cases where the Agency has made changes to sections we have previously discussed, we build upon those recommendations below.

There is one concern we outlined in previous comments that has not been addressed in the latest version of the draft rules. Section 7016 addresses financial incentives that businesses offer to consumers to hand over their personal information to the business. This practice is commonly referred to as “pay-for-privacy,” as the net effect on the consumer is often paying a higher price for a good or service if they choose to make the privacy-protective choice.

We remain disappointed that draft regulations leave mostly untouched the extreme license given to businesses to compute “the value of the customer’s data” according to almost any formula or method that they might choose. The lack of specific guidance will likely result in a crazy-quilt of methods to measure the value of the customer’s data to the business. The statute requires the incentive to be “reasonably related” to the figure the company provides, but these regulations fail to provide a standard to ensure that the value number itself is reasonable. Thus, these regulations leave room for companies to come up with figures that may be completely unreasonable values for customers’ data so long as the financial incentive the company provides is reasonably related to the unreasonable value the company gives the

Group Comments

Comments on Modified Text of Proposed Regulations

Page 5 of 14

data. For a financial incentive to be reasonably related to an unreasonable value computation seems neither reasonable nor protective to consumers.

We reiterate our recommendation that the Agency consider providing some sample computations of the value of a consumer's data to a business, as you have provided examples in a number of other sections of the draft regulations. The examples can and should include an example of a reasonable method to arrive at a value number as well as an example of an unreasonable method.

Such examples should also include acceptable additional business purposes for acquired customer data that clearly meet the "reasonable consumer expectation" standard and examples of those that would not meet the "reasonable consumer expectation" standard.

### **Comments on New Changes To Regulations Published On Nov. 8, 2022**

As privacy advocates, we are concerned about several changes to the regulations that appear to set up additional barriers to consumers' ability to exercise their rights under the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA).

#### **Changes to Definition of "Disproportionate effort"**

Changes to the definition of "disproportionate effort" will make it easier for businesses to refuse to fulfill valid consumer requests to know and correct information, and to refuse to pass those requests on to third parties with which they have shared information. In our previous comments, we asked that this definition be changed to prevent people being put in a situation where a business defines what "benefit" such a request may provide to them.

The updated definition shifts the balance of power even more in favor of businesses by allowing businesses to decline to comply with requests based on their evaluation of the

"reasonably foreseeable impact to the consumer by not responding." It also remains unclear to us what the consumer's appeal rights will be when a business informs a consumer that their request will not be fulfilled because the effort to the business is disproportionate to the benefit they will receive.

### **The Removal of Illustrative Examples in § 7002(b)**

During the written comment period for the first draft of these Regulations we applauded the Agency for including illustrative examples throughout the draft that clearly indicated the Agency's intent and provided well defined guard-rails for businesses to follow. The removal of illustrative examples in § 7002(b) makes it easier for businesses to mislead and confuse consumers, reduces the clarity of the regulations, and weakens the protections of the CCPA.

Where there was a clear standard based on a reasonable consumer's reasonable expectations and a series of examples indicating what violations of that expectation could look like, now there are multiple multi-element tests that still leave as much in question as a reasonableness standard. Relying on, for example, "the strength of the link" between a consumer's reasonable expectations at the time of collection and "the other disclosed purposes" requires the same reasonableness analysis, but introduces an additional layer of uncertainty, compounded by the lack of clear illustrative examples of what could constitute a violation. In light of their inclusion and subsequent removal from the draft it also introduces confusion as to whether the Agency considers, for example, a mobile flashlight application that collects consumer geolocation information without the consumer's explicit consent to be in accordance with the section 7002 restrictions on collection and use.

Illustrative examples provide concrete representations of the regulations as applied, a crucial illustration of the Agency's intent, and in many cases were based on real-world

Group Comments

Comments on Modified Text of Proposed Regulations

Page 7 of 14

privacy-invasive business practices that these regulations are attempting to address.<sup>1</sup> We urge the agency to reinstate the illustrative examples that were removed in section 7002(b).

### **The removal of illustrative examples in § 7004(a)(2)**

The removal of the illustrative examples in § 7004(a)(2)(D) & (E), has the effect of significantly weakening the principle of “symmetry of choice” and striking an essential category of dark patterns.

As defined in the OECD’s report on *Dark Commercial Patterns*: “**Interface interference**: . . . [gives] visual precedence to options favourable to the business, thus creating a false hierarchy.”<sup>2</sup> § 7004(a)(2)(D) & (E) are examples of interface interference giving visual precedence to more favorable business options, and further, explicitly illustrated how “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”. The removed illustrative examples could just as easily be considered “preselection variants” of the “Asymmetric Choice” dark pattern outlined by the FTC staff report, *Bringing Dark Patterns to Light*.<sup>3</sup>

Striking these examples is antithetical to the findings, intents and purposes of the CPRA ballot initiative as well, which acknowledged that information asymmetry makes it difficult for consumers to “at a glance” understand what they are exchanging and therefore difficult or impossible to negotiate with businesses; that businesses and consumers should be

---

<sup>1</sup> Federal Trade Commission, *Android Flashlight App Developer Settles FTC Charges It Deceived Consumers*, (Dec. 5, 2013) available at <https://www.ftc.gov/news-events/news/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived-consumers>.

<sup>2</sup> OECD, *Dark Commercial Patterns*, OECD Digital Economy Papers, 10 (Oct. 2022), available at [https://www.oecd-ilibrary.org/science-and-technology/dark-commercial-patterns\\_44f5e846-en](https://www.oecd-ilibrary.org/science-and-technology/dark-commercial-patterns_44f5e846-en).

<sup>3</sup> Federal Trade Commission, *Bringing Dark Patterns to Light*, 25 (Sept. 14, 2022), [https://www.ftc.gov/system/files/ftc\\_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf).



Group Comments

Comments on Modified Text of Proposed Regulations

Page 8 of 14

given clear guidance about their responsibilities and rights; and that the law should empower the consumer to be able to negotiate with the business on equal footing.<sup>4</sup>

Allowing businesses to preselect a “yes” choice or more prominently display the choice to participate in a financial incentive program will compound the problems identified above, make it easier for businesses to mislead consumers, undermine the intent of the ballot initiative, and would be a significant weakening of these Regulations from the first draft. For these reasons and others we urge the agency to reinstate the removed illustrative examples from § 7004(a)(2).

**Changes to § 7004(a)(4) reduces clarity and significantly weakens the protections against dark patterns.**

In § 7004(a)(4), removing “manipulative language” is antithetical to the spirit of the section and the CCPA. “Manipulation” has been a critical component of dark patterns since the term’s inception. From the FTC’s *Bringing Dark Patterns to Light*, “Coined in 2010 by user design specialist Harry Brignull, the term ‘dark patterns’ has been used to describe design practices that trick or manipulate users into making choices they would not otherwise have made and that may cause harm.”<sup>5</sup> By only prohibiting language that would “impair or interfere” consumers’ choice, it removes a class of dark patterns that are designed to nudge, manipulate, or influence. For example, in the Norwegian Consumer Council’s report *Deceived by Design*, they detail Facebook’s attempt to roll out face recognition technology by highlighting all of the positive sides of data sharing when prompting users to give their

---

<sup>4</sup> The California Privacy Rights Act, SEC. 2(F), (H); see also SEC. 3(B)(1), (C)(2),(3).

<sup>5</sup> *Bringing Dark Patterns to Light*, *supra* note 3, 2.

Group Comments

Comments on Modified Text of Proposed Regulations

Page 9 of 14

consent. On the flip side, Facebook framed opting-out of data sharing as dangerous or risky.<sup>6</sup>

As written, the regulations would not cover this type of dark pattern.

Instead, the Agency would have to rely on § 7004(c) to determine whether this practice is “substantially subverting or impairing user autonomy” as a backstop, undermining the clarity and proactivity that the regulations are meant to provide. Disconnecting this principle from the concept of manipulation will make it easier for businesses to use dark patterns and mislead consumers. We urge the Agency to recenter the concept of “manipulation” in § 7004(a)(4).

**§ 7004(c). Requiring a business’s intent to be a factor that must be considered in determining whether a user interface is a dark pattern is costly and reduces clarity of the regulations.**

Adding business intent in § 7004(c) as a factor creates a larger administrative burden for the Agency, as the Agency would presumably need access to the organization’s emails, meeting minutes, and other documents in its attempt to construct intent. It also incorrectly shifts the focus from a practice’s impact on end-users to a business’s culture and internal procedures.

Additionally, development of dark patterns is increasingly being done without any human interaction: “[B]usinesses are moving toward the use of artificial intelligence both to design and target digital materials. At some point, no human will need to be directly involved. The only discernible business intent is likely to be intent to maximize business

---

<sup>6</sup> Norwegian Consumer Council, *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy* (Jun. 27, 2018), 22, available at <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-designfinal.pdf>.

Group Comments

Comments on Modified Text of Proposed Regulations

Page 10 of 14

metrics such as click rates, sales, or retentions. No human needs to intend to deceive or know that the design is deceptive.”<sup>7</sup>

### **§ 7011. Privacy Policy**

We had not previously provided comment on the changes to this section, which significantly weakened the ability for all people to access and understand business privacy policies. The Agency previously did considerable work to ensure that every consumer, regardless of their ability or language skill, would have a reasonable chance of being able to access and understand these policies. To only require that it be in a format that "allows a consumer to print it out as a document" is a major step back from the goals of accessibility laid out in the original rules.

### **Removing Requirements to Notify Consumers About Third Parties at Point of Collection and Requirements to Notify Third Parties About Consumer Requests.**

The latest draft of regulations remove an obligation for businesses to notify people about which third parties the business allows to control personal information. These regulations also, at several points, weaken or remove requirements for businesses to notify third parties about consumer requests—particularly requests to opt out of sale and sharing, requests to limit the use of sensitive personal information, and requests to delete information. While the Agency has pointed to revisions of §7052 and §7053 as the reason for these changes, we respectfully disagree that those sections serve the same utility to consumers as those that have been altered or removed.

Removing the §7012(e)(6) obligation for businesses to notify consumers at the point of collection about which third parties may also control their data, or information about their

---

<sup>7</sup> Lauren E. Willis, *Deception by Design*, 34 Harv. J. Law & Tech. 115, 158 (2020).

business practices, makes it substantially more difficult for any consumer to understand what will happen with their information after it is collected. Transparency is the first step toward empowering consumers to exercise their privacy rights. The CCPA and the CPRA, in a majority of circumstances, already place the onus on consumers to seek out and file requests with every company that may hold their information. Removing this notice makes this process an even more burdensome guessing game for consumers.

Furthermore, responsible businesses that properly safeguard consumer data should know how information they collect flows to third parties. Stating this at the point of collection should not be difficult for businesses, and doing so makes exercising rights substantially easier for consumers.

Additionally, changes to §7022 (b, c) could narrow the instances in which businesses must notify service providers or contractors about consumer deletion requests. Rather than covering any information "obtained in the course of providing services," the draft rules now only cover information that is specified in a written contract between businesses and their service providers or contractors, or that businesses have "enabled" these third parties to collect.

In its explanation of the change, the Agency notes that this alters the "language to be more precise about how the service provider's or contractor's obligations apply to the personal information it collected pursuant to the written contract with the business." This narrowing, however, potentially allows for third parties to retain information they may collect in the course of doing business but that is not specifically enumerated in any written agreement, even in light of a deletion request.

Of perhaps greater concern are changes to §7026(f)(2) and §7027 that remove any requirement to notify third parties of requests to opt out of sale or sharing, or to limit the use of sensitive personal information. As already noted, the CCPA and CPRA already do not

provide many mechanisms to make it easier for consumers to exercise their rights. These changes further exacerbate this issue by requiring consumers to file even more requests to safeguard and exert control over their own information. Businesses, by the nature of the contractor or service provider relationship, have both a knowledge of which third parties they share information with, and a means of communicating with those third parties. Consumers have neither.

These changes will allow businesses to obscure how consumer information flows through any number of companies and make it significantly more difficult for consumers to exercise their rights under the CCPA and CPRA. It places a significantly greater burden on consumers who wish to safeguard their privacy. Indeed, the combination of being required to file duplicative requests with each separate entity and being kept in the dark about which companies control their data in the first place may make it impossible for many consumers to exercise their rights at all.

### **§ 7023. Requests to Correct.**

In §7023, as elsewhere in the draft regulations, the Agency has potentially narrowed the instances in which a business must pass on requests—in this instance, to correct information, which raise concerns that businesses may leave uncorrected any information that is not specifically mentioned in a written contract, even if a consumer requests it be corrected. The draft regulations have also removed several illustrative examples from this section, which provided clear and valuable guidance about how this new right should be implemented.

We also do not understand the addition, in §7023(d)(1), of a requirement for consumers to make a "good-faith effort to provide businesses with all necessary information available at the time of the request." This provision will require more clarification for

consumers to be able to comply with it. As written, it could prevent consumers from being able to exercise this right at all. Consumers often will not know what kind of information a business may deem necessary to make a correction request.

We also would oppose any effort from business to raise this bar so high that no average consumer would be able to demonstrate a "good-faith" effort. Some businesses have already required processes that are far more rigorous than is necessary to comply with CCPA requests—such as requesting notarization or signing an affidavit to verify people's identities to fulfill requests.<sup>8</sup> As such, more specificity about what constitutes a "good-faith" effort would aid consumers in understanding their own obligations.

**§ 7025. The Regulations Inappropriately Permit Dark Patterns when processing in a “nonfrictionless manner”**

We have previously objected to the concept of permitted “non-frictionless processing” under section 7025(e), wherein businesses are expressly authorized to introduce any of the dark patterns outlined in 7004 - characterized as “friction” - when processing an opt-out preference signal, as long as they also include a “Do Not Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” link on the business’s homepage.

This framework threatens to make the opt-out preference signals an unusable mechanism to communicate a consumer’s privacy choices, with businesses able to rely on practices that this Agency acknowledges subvert user autonomy and has the effect of manipulating consumers. Interface interference and asymmetric choices with privacy-invasive options selected by default, coerced actions nagging users that have enabled opt-out preference signals, and pop-up text, graphic animation, sound and video content will be used

---

<sup>8</sup> Margaret Oates, *Identity verification: flows we’ve seen in CCPA data requests*, Consumer Reports (July 2022) <https://digital-lab-wp.consumerreports.org/2022/07/07/identity-verification-flows-weve-seen-in-ccpa-data-requests-2-of-2/>.

Group Comments

Comments on Modified Text of Proposed Regulations

Page 14 of 14

to discourage consumers from using opt-out preference signals. What should be a mechanism to seamlessly and frictionlessly communicate a consumer's right to exercise privacy choices will instead open up the consumer to the same kinds of abusive practices that are otherwise prohibited by the CCPA. Permitting this kind of mischief is inconsistent with both the explicit mandate of the statute, which does not permit dark patterns in response to opt-out preference signals, and the intent of the ballot initiative, which is to increase opt-out preference signal protections under California law.

Respectfully Submitted,

Emory Roane, Privacy Rights Clearinghouse

Halyley Tsukayama, Electronic Frontier Foundation

Becca Cramer-Mowder, ACLU California Action

Jacob Snow, ACLU California Action

Tracy Rosenberg, Oakland Privacy and Media Alliance

Susan Grant, Consumer Federation of America

---

**From:** Parker, Sarah [REDACTED]  
**Sent:** Monday, November 21, 2022 7:57 AM  
**To:** Regulations  
**Subject:** CPPA Public Comment  
**Attachments:** BPI Comments on Modified Proposed Rules\_11.21.2022.pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

To whom it may concern:

On behalf of Gregg Rozansky and the Bank Policy Institute, please find attached comments on the Modified Proposed Regulations implementing the CPRA. Thank you.

Best,  
Sarah

**Sarah Parker**  
Pronouns: She/Her/Hers  
Covington & Burling LLP  
One CityCenter, 850 Tenth Street, NW  
Washington, DC 20001-4956  
[REDACTED]

[www.cov.com](http://www.cov.com)

**COVINGTON**

---

This message is from a law firm and may contain information that is confidential or legally privileged. If you are not the intended recipient, please immediately advise the sender by reply e-mail that this message has been inadvertently transmitted to you and delete this e-mail from your system. Thank you for your cooperation.





November 21, 2022

*Via electronic mail*

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

Re: **Modified Proposed Regulations Under the California Consumer Privacy Act**

The Bank Policy Institute (BPI)<sup>1</sup> appreciates the opportunity to submit comments to the California Privacy Protection Agency on the Modified Proposed Regulations implementing the California Consumer Privacy Act, as amended by the California Privacy Rights Act.<sup>2</sup>

**I. Executive Summary**

BPI's members are financial institutions that have invested significant time and resources into building data protection and information security compliance systems that align with federal and state financial privacy laws. BPI members are committed to promoting robust privacy protections for California consumers.

Drawing on the experience of its members operationalizing privacy and security safeguards for their customers, BPI previously submitted comments on the initial Proposed Regulations implementing the CCPA.<sup>3</sup> Many of these comments relate to three key themes:

- First, the regulations should embody standards that are sufficiently flexible to enable businesses to promote consumer privacy effectively. Consumers are not always served by lengthy and technical disclosures or overly prescriptive requirements.
- Second, the regulations must operate within the parameters established by the legislature and California voters.

---

<sup>1</sup> The Bank Policy Institute is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost two million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.

<sup>2</sup> Cal. Civ. Code § 1798.100 *et seq.*

<sup>3</sup> See Letter from BPI to California Privacy Protection Agency, Re: Proposed Regulations Under the California Consumer Privacy Act (Aug. 23, 2022).

- Third, the regulations should recognize the critical role of other federal and state privacy and consumer protection frameworks in protecting consumers.

We commend the Agency for amendments it made to the Modified Proposed Regulations in service of these goals, although, as discussed further below, we urge the Agency to go further and address recommended changes that have not yet been addressed.

Today, BPI emphasizes a small number of technical corrections and clarifications that are necessary to avoid seemingly unintended consequences. In addition, BPI is writing to urge the Agency to delay enforcement as it relates to employee and business-to-business (“B2B”) personal information. The Agency should not enforce general consumer data protection rules in the employment and B2B contexts without careful consideration of their impact and analysis of employment laws, existing commercial contracts, and other legal frameworks. Finally, BPI also reiterates its prior comments, including by urging the Agency to move away from highly prescriptive requirements for contracts with service providers and third parties.

## II. Additional Technical Corrections and Clarifications Are Necessary.

In this Section, we identify several technical corrections and clarifications that are “low-hanging fruit” for the Agency to remedy. It is not clear that the Agency intends the harmful implications described below, and, in any event, these corrections are important to serve the statutory goals of “strengthening consumer privacy, while giving attention to the impact on business and innovation.”<sup>4</sup>

### a. Notice at Collection – Modified Proposed Regulations § 7012(f)

Section 7012(f) requires a business that collects personal information online to provide the notice at collection by providing a “link that takes the consumer *directly* to the specific section of the business’s privacy policy that contains the information required in subsection (e)(1) through (6).” The section continues by stating that directing the consumer to the beginning of the privacy policy, or to any other section without the required information, will not satisfy the notice at collection requirement.

This requirement is overly prescriptive, burdensome, and impracticable, particularly for financial institutions that are managing disclosures to consumers that comply not only with a constellation of general privacy laws, but also federal and state financial privacy laws. While some businesses rely on an online privacy policy to provide a notice at collection, other businesses elect to link within their online privacy policy or a privacy center page to a California-specific notice to address the required disclosures. So long as businesses ensure that consumers have ready access to the relevant information, businesses should have the flexibility to deliver information to consumers based on the clearest presentation to the users.

---

<sup>4</sup> The California Privacy Rights Act of 2020, Cal. Prop. 24 § 3(C)(1) (2020); *see also* Cal. Civ. Code § 1798.199.40(l) (instructing the Agency to “seek to balance the goals of strengthening consumer privacy while giving attention to the impact on businesses”).

Detailed prescriptions on the layering and organization of content within privacy notices are not necessary given that the Modified Proposed Regulations elsewhere address requirements to ensure that notices are provided conspicuously, *see* § 7003, and to ensure that consumers understand the choices available to them, *see* § 7004. Further, this level of prescription raises constitutional and administrative legal questions by burdening the ability of businesses to use a single interface to interact with users across states without directing non-California consumers *directly* to a California-specific privacy notice. Generalizing this requirement would permit businesses greater latitude to communicate effectively with consumers, both Californians and non-Californians alike.

We recommend deleting this provision or, in the alternative, making edits to remove the requirement to link directly to the *specific* section of the privacy policy that contains the required terms. Proposed language can be found in Appendix A to this letter.

b. Third Party Contracts – Modified Proposed Regulations § 7052(a)

We commend the Agency on edits that it has made to Sections 7052 and 7053, which bring the regulations closer to alignment with the statutory requirements for third parties, although, as described below, we continue to have concerns with some of the elements of the Modified Proposed Regulations. We also think that minor, clarifying edits are necessary for the new Section 7052(a), which reads that, “[a] third party that does not have a contract that complies with section 7053, subsection (a), shall not collect, use, process, retain, sell, or share the personal information that the business made available to it.”

At best, this is not drafted clearly. At worst, it seems to contemplate a contract between businesses and *every* third party—not just those to which personal information is sold or shared. Such a requirement is not consistent with the statutory design.<sup>5</sup> It also would limit consumers’ control over their personal information, as it would limit the disclosure of personal information by a business to a third party in circumstances in which a consumer directs the business to intentionally disclose the information. In such a case, the recipient would be prohibited from collecting the personal information made available to it.

We recommend amendments to clarify that the provision only applies to third parties to which personal information is sold or shared. Proposed language can be found in Appendix A to this letter.

c. Requests to Know – Modified Proposed Regulations § 7024(h)

We continue to have concerns about Section 7024(h) of the Modified Proposed Regulations, even after the Agency’s modifications. The section contemplates that businesses, in response to a request to know, will provide all personal information collected or maintained about the consumer on or after January 1, 2022, including *beyond the 12-month period* before the

---

<sup>5</sup> *See* Cal Civ. Code 1798.100(d) (contemplating contracts between businesses and third parties to which personal information *is sold or shared*).

receipt of the request, unless the consumer requests data for a specific time period or doing so proves impossible or would involve disproportionate effort. In contrast, the plain language of the statute contemplates that businesses will provide information for a 12-month period unless consumers request additional information beyond the 12-month period.<sup>6</sup>

In its initial Explanation of Modified Text of Proposed Regulations, the Agency recognized the need to “conform the regulation to the language of Civil Code § 1798.130(a)(2)(B).” However, the Modified Proposed Regulations still do not address the 12-month look-back period in a manner consistent with the statutory text. To ensure consistency with the statute, the Proposed Rules should be clear that there is no requirement to provide information beyond the 12-month period unless the consumer specifically requests it.

We recommend amendments to conform with the statutory text by specifying that a business must provide information only for the 12-month period preceding the request, unless the consumer requests otherwise. Proposed language can be found in Appendix A to this letter, which mirrors the changes that we recommended in our letter dated August 23, 2022.

### **III. Enforcement Should Be Delayed For Employee and Business-to-Business Personal Information.**

As described below, the Agency should move forward with providing clearer guidance with respect to employee and B2B personal information. In the meantime, however, the Agency should clarify that the CCPA and its implementing regulations will not be enforced with respect to employee and B2B personal information.

The wholesale importation of general consumer protection principles to the employee and commercial context fails to account for important differences between a business’s relationship with traditional consumers, as compared to those with whom a business interacts in an employment or commercial context. Not only are expectations of privacy significantly different in the employment and commercial contexts, but these areas already are heavily regulated. Indeed, there are federal and state laws that reflect policy judgments about the rights that job applicants and employees should have to access their personnel records and similar personal information.<sup>7</sup> These legal frameworks reflect relevant policy judgments that the CPRA should not be construed to displace in the absence of more clear intent. For example, Cal. Lab. Code § 1198.5 includes various exceptions to the circumstances in which employers must afford employees with access to their personnel records, including in the context of a lawsuit filed by a current or former employee that relates to a personnel matter against the employer.

---

<sup>6</sup> See Cal. Civ. Code § 1798.130(a)(2)(B) (“The disclosure of the required information shall cover the 12 month period preceding the business’s receipt of the verifiable consumer request, provided that, upon the adoption of a regulation pursuant to paragraph (9) of subdivision (a) of Section 1798.185, a consumer may request that the business disclose the required information beyond the 12 month period and the business shall be required to provide such information unless doing so proves impossible or would involve a disproportionate effort.”).

<sup>7</sup> See Cal. Lab. Code § 1198.5; Cal. Lab. Code § 226(b); Cal. Lab. Code § 432; Cal. Civ. Code § 1786 *et seq.*; and Cal. Civ. Code § 1786.53.

Likewise, the CPRA should not be construed to displace or interfere with rights and obligations governed by commercial business relationships absent clear intent to do so. Yet, this would be the practical impact of the currently contemplated application of wholesale general consumer protection principles to the commercial context without clear guidance that accounts for important differences between a business' relationships with its customers in these context.

For these reasons, we appreciate comments made during the October 28 and 29, 2022 Board meetings relating to the importance of the Agency providing clear guidance and exceptions for the employee and B2B contexts. When the Agency provides more specific guidance on these issues, BPI's members are happy to work with the Agency to provide further comments about the application of the CPRA in these contexts. Among other important points, the Agency should ensure that its rules are consistent with other relevant legal frameworks and construe the "specific pieces" of personal information definition appropriately to exclude, for example, confidential business information and internal business records and communications.

In the meantime, until the Agency is able to provide more specific guidance, the Agency should make clear that the CCPA should not be enforced in respect of employee and business customer data. The statute affords the Agency the discretion to treat employee and business customer data differently. Indeed, the statute makes clear that the privacy interests of employees should be protected "taking into account the differences in the relationship between employees or independent contractors and businesses, as compared to the relationship between consumers and businesses."<sup>8</sup> The ballot initiative also specifies that the law is not intended to interfere with other laws, such as the National Labor Relations Act ("NLRA").<sup>9</sup> And, more generally, the ballot initiative makes clear that "[b]usinesses and consumers should be provided with clear guidance about their responsibilities and rights."<sup>10</sup> This provides ample basis for the Agency to delay application of the CCPA with respect to employee and business customer data.

Conversely, long-standing principles of administrative law preclude the Agency from adopting rules without such a provision in the absence of full consideration of the implications. At present, the current record fails to reflect consideration of the impact of applying various regulatory requirements to employee and B2B personal information. For example, Section 7027(m) lists "[t]he purposes. . . for which a business may use or disclose sensitive personal information without being required to offer consumers a right to limit[.]" However, none of the eight examples seem to contemplate processing activities that would be relevant for employee or business-to-business data.

---

<sup>8</sup> The California Privacy Rights Act of 2020, Cal. Prop. 24 § 3(A)(8) (2020).

<sup>9</sup> *Id.*

<sup>10</sup> *Id.* § 3(C)(2). Unlike the CCPA, the other comprehensive state privacy laws exempt employee and business-to-business data, recognizing that there are fundamentally different considerations at play with respect to this data. *See, e.g.,* Va. Code Ann. § 59.1-571 (definition of "consumer" exempts "a natural person acting in a commercial or employment context"); Colo. Rev. Stat. § 6-1-1303(6) (definition of "consumer" "does not include an individual acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context").

Further, the record also does not reflect any consideration of the potential economic impact of extending various provisions in the employment and business customer context, including as it relates to the economic burden where there is tension between confidentiality obligations owed to a business customer and privacy rights of their personnel. These economic impacts are exacerbated given the context: until the end of its legislative session on August 1, the California legislature was still considering bills that would have extended the exemptions.<sup>11</sup> And the CCPA has emerged as an outlier in the U.S. in terms of its treatment of employee and B2B personal information.<sup>12</sup>

In order to resolve these issues, the Agency should clarify that the CCPA and implementing regulations will not be enforced with respect to employee and B2B personal information until the Agency has a chance to review the final regulations and implement appropriate exceptions. At a minimum, the Agency should ensure that the regulations specify that enforcement must account for the lack of clear guidance with respect to employee and business-to-business personal information. Proposed language can be found in Appendix A to this letter.

#### **IV. BPI's Prior Comments Should Also Be Considered Before Finalizing the Rules.**

Finally, we urge the Agency to address recommended changes from BPI's August 23, 2022 comment letter that have not yet been addressed. The changes that the Agency made in response to BPI's prior comment letter are positive in better aligning the Modified Proposed Regulations with business incentives to better protect consumers, including by removing certain detailed technical requirements that lacked any tangible consumer benefit. For example, we commend the change the Agency made to remove the arbitrary five-day requirement for service providers to notify a business in the event a service provider can no longer meet its obligations. However, we urge the Agency to revisit those recommendations it has not yet addressed, particularly as it relates to prescriptive contract requirements and mandatory requirements to honor a global opt-out preference signal.

a. Contract Requirements – Modified Proposed Regulations §§ 7051(a)(2), 7053(a)(1)

The Modified Proposed Regulations retain requirements of Section 7051(a)(2) that requires businesses to identify, in each service provider or contractor agreement, the specific business purpose(s) for which personal information is disclosed, and prohibits use of generic language in doing so. Similar language appears in Section 7053(a)(1). These prescriptive contract requirements go beyond the obligations in the statute. There should be a high bar before the Agency adopts new requirements that are not grounded in the statutory text, particularly given that many businesses have already adapted their contracts multiple times to adhere to the evolving requirements set out in the CCPA and its implementing regulations. This bar is not met here, where the additional requirements will confer minimal incremental benefit to consumers while imposing a substantial burden on both businesses and their service providers.

---

<sup>11</sup> See A.B. 2871, Cal. Assembly (2021–2022); A.B. 2891, Cal. Assembly (2021–2022).

Further, these requirements deviate from, and therefore make the CCPA framework less interoperable with, other federal, state, and international privacy laws. This issue is particularly salient for banks, which retain service providers to support activities that do not just involve the processing of personal information subject to the CCPA—but also involve the processing of nonpublic personal information subject to the Gramm-Leach-Bliley Act’s (“GLBA”) separate requirements for contractual agreements with service providers.<sup>13</sup> For more information on these concerns, we refer the Agency to our additional analysis on contractual requirements in Section 3(a) of our comments dated August 23, 2022.

In addition, we recommend deleting both of these sections in full or, in the alternative, deleting the language requiring a “specific” rather than “generic” description of the business purposes. Proposed language can be found in Appendix A to this letter.

b. Opt-Out Preference Signals – Modified Proposed Regulations § 7026(a)

The requirements relating to opt-out preference signals should be consistent with the statutory design, which affords businesses flexibility as to whether to honor such signals or post a link on their home page.<sup>14</sup> In any event, to the extent some businesses honor opt-out preference signals, the Modified Proposed Regulations should be clear and consistent in terms of the relevant requirements, including by addressing the comments we provided in Section 3(c) of our comments dated August 23, 2022.

More broadly, we urge the Agency to further consider BPI’s recommendations that were not addressed in full as part of the edits made to the Modified Proposed Regulations on July 8, 2022. For ease of review, we refer the Agency to Appendix A of our comments dated August 23, 2022. This appendix contains a set of proposed amendments that BPI continues to urge the Agency to adopt, together with the additional amendments included as Appendix A to today’s comment letter.

\*\*\*\*\*

The Bank Policy Institute appreciates the opportunity to submit comments on the Agency’s Modified Proposed Regulations implementing the CPRA. If you have any questions, please contact the undersigned by phone at [REDACTED] or by email at [REDACTED]

Respectfully submitted,

[REDACTED]  
Gregg Rozansky  
Senior Vice President

---

<sup>13</sup> See, e.g., 12 C.F.R. § 1016.13(a). Banks are also subject to broader third-party risk management guidance issued by banking regulators.

<sup>14</sup> Cal. Civ. Code § 1798.135(a)–(b).

Senior Associate General Counsel  
Bank Policy Institute



**Appendix A**

*Gray rows provide detail on points made in Parts II, III, and IV. White rows include additional examples and/or points not addressed in Parts II, II, and IV.*

| Citations   | Comment  | Proposed Redline to Cited Modified Proposed Regulations Provision  |
|---|--|--|
| <b>Section II – Technical Corrections and Clarifications</b>                          |  |  |
| <p>Modified Proposed Regulations § 7012(f)</p> <p>Cal. Civ. Code § 1798.100(a)(1)</p> | <p>Section 7012(f) requires a business that collects personal information online to provide the notice at collection by providing a “link that takes the consumer directly to the specific section of the business’s privacy policy that contains the information required in subsection (e)(1) through (6).” This requirement is overly prescriptive, burdensome, and impracticable, particularly for financial institutions that are managing disclosures to consumers that comply not only with a constellation of general privacy laws, but also federal and state financial privacy laws.</p> | <p><i>Delete § 7012(f).</i></p> <p><i>In the alternative, amend § 7012(f):</i></p> <p>“If a business collects personal information from a consumer online, the Notice at Collection may be given to the consumer by providing a link <del>that takes the consumer directly</del> to the <del>specific section of the</del> business’s privacy policy that contains the information required in subsection (e)(1) through (6). <del>Directing the consumer to the beginning of the privacy policy, or to another section of the privacy policy that does not contain the required information, so that the consumer is required to scroll through other information in order to determine the categories of personal information to be collected and/or whether the business sells or shares the personal information collected, does not satisfy this standard.</del>”</p> |
| <p>Modified Proposed Regulations § 7052(a)</p> <p>Cal. Civ. Code § 1798.100(d)</p>    | <p>The modified Section 7052(a) reads that, “[a] third party that does not have a contract that complies with section 7053, subsection (a), shall not collect, use, process, retain, sell, or share the personal information that the business made available to it. This is unclear in that it could be read to contemplate a contract between businesses and <i>every</i> third party—not just those to which personal information</p>   | <p><i>Amend § 7052:</i></p> <p>§ 7052. Third Parties</p> <p>“(a) A third party <u>to which personal information is sold or shared</u> that does not have a contract that complies with section 7053 subsection (a) in respect of such personal information, shall not collect, use, process, retain, sell, or share the personal information that the business made available to it.</p> <p>(b) A third party shall <del>comply with the terms of the contract required by the</del></p>   |

| Citations   | Comment  | Proposed Redline to Cited Modified Proposed Regulations Provision  |
|---|--|--|
|   | <p>is sold or shared. Such a requirement is not consistent with the statutory design and would limit consumers’ control over their personal information.</p>   | <p><del>CCPA and these regulations, which include treating</del> the personal information that the business made available to it in a manner consistent with the <del>business’s</del> <u>third party’s</u> obligations under the CCPA and these regulations.”</p>   |
| <p>Modified Proposed Regulations § 7024(h)<br/><br/>Cal. Civ. Code §§ 1798.130(a)(2)(B), 1798.185(a)(9)</p> | <p>The Proposed Regulations do not address the 12-month look-back period for consumer requests in a manner consistent with the statutory text. Consumers should be permitted to request older information from businesses, but the rules should not impose a mandatory requirement that businesses <i>shall</i> affirmatively provide the information.</p> | <p><i>Amend § 7024(h):</i></p> <p>“In response to a request to know, a business shall provide all the personal information it has collected and maintains about the consumer <u>for the 12-month period preceding the business’s receipt of the verifiable consumer request. A consumer may request that the business provide all the personal information it has</u> on or after January 1, 2022, including beyond the 12-month period preceding the business’s receipt of the request, unless doing so proves impossible or would involve disproportionate effort, <del>or the consumer requests data for a specific time period. The</del> <u>at information to be provided</u> shall include any personal information that the business’s service providers or contractors Collected pursuant to their written contract with the business. If a business claims that providing personal information beyond the 12-month period would be impossible or would involve disproportionate effort, the business shall provide the consumer <del>an</del> <u>detailed</u> explanation <del>that includes enough facts to give a consumer a meaningful understanding as to why the business cannot provide personal information beyond the 12-month period</del> <u>for its decision. The business shall not simply state that it is impossible or would require disproportionate effort.</u>”</p> |
| <p>Modified Proposed Regulations §§ 7022(d),</p>  | <p>Section 7022(d) states that a business that stores any personal information on archived or back-up systems</p>  | <p><i>Amend § 7022(d) and 7023(c) either in line with our proposed edits in Appendix A of our letter dated August 23, 2022 or, at a minimum, in line with the below:</i></p>   |

| Citations  | Comment  | Proposed Redline to Cited Modified Proposed Regulations Provision  |
|--|--|--|
| <p>7022(b)(1),<br/>7023(c)</p> <p>Cal. Civ. Code §§<br/>1798.105(c),<br/>1798.106(c)</p>                               | <p>“may delay compliance with the consumer’s request” until the archived or back-up system is “restored to an active system or is next accessed or used for a sale, disclosure, or commercial purpose.” Clarifications are needed to align this provision with 7022(b)(1), which does not require businesses to delete a consumer’s personal information from “archived or back-up systems.” Section 7023(c) also contains similar contradictions tied to correction rights.</p> | <p>§ 7022. Requests to Delete</p> <p>“(d) If a business, service provider, or contractor stores any personal information on archived or backup systems, it may delay compliance with the consumer’s request to delete, with respect to data stored on the archived or backup system, until the <u>relevant data is restored from the archived or backup system</u> <del>relating to that data is restored</del> to an active system or is <del>next accessed or</del> used for a sale, disclosure, or commercial purpose.”</p> <p><i>Apply corresponding edits to similar language in Section 7023(c).</i></p>   |
| <p><b>Section III – Employee and B2B Data</b></p>  |  |  |
| <p>Modified Proposed Regulations § 7301</p> <p>Cal. Civ. Code §§<br/>1798.155,<br/>1798.199.40(a),<br/>1798.199.45</p> | <p>Applying the CCPA and its regulations to employee and business-to-business personal information will create unintended consequences and compliance problems not easily solved without further guidance and clarity. At a minimum, the agency should ensure that enforcement must account for the lack of clear guidance until it can adopt and clarify appropriate standards.</p>   | <p><i>Amend § 7301:</i></p> <p>§ 7301 Investigations.</p> <p>“(c) For personal information that is <u>described in Civil Code section 1798.145, subdivision (m) or subdivision (n), the Agency shall not begin enforcement of possible or alleged violations of the CCPA until the Agency has promulgated additional regulations addressing businesses’ obligations with respect to these categories of personal information.</u>”</p> <p><i>In the alternative, amend § 7301 as follows:</i></p> <p>§ 7301 Investigations.</p> <p>“(c) For personal information that is <u>described in Civil Code section 1798.145, subdivision (m) or subdivision (n), the interpretation of the CCPA and investigations of possible or alleged violations of the CCPA will take into</u></p> |

| Citations  | Comment  | Proposed Redline to Cited Modified Proposed Regulations Provision   |
|--|--|---|
|  |  | <p><a href="#">account good faith efforts to comply and the lack of clear statutory and regulatory requirements and expectations.”</a></p>  |
| <p><b>Section IV – BPI’s Prior Comments</b></p>  |  |   |
| <p>Modified Proposed Regulations §§ 7051(a)(2), 7053(a)(1)</p> <p>Cal. Civ. Code §§ 1798.100(d), 1798.140(e)(5), (j), (ag)</p> | <p>Section 7051(a)(2) requires businesses to identify, in each service provider or contractor agreement, the specific business purpose(s) for which personal information is disclosed, and prohibits use of generic language in doing so. This goes beyond the obligations in the statute and would require an impracticable amount of contract remediation. Section 7053(a)(1) of the draft regulations requires comparable information for third party agreements.</p> | <p><i>Delete §§ 7051(a)(2) and 7053(a)(1).</i></p> <p><i>In the alternative and at a minimum, amend § 7051(a)(2):</i></p> <p>“Identify the specific Business Purpose(s) for which the service provider or contractor is processing personal information pursuant to the written contract with the business, and specify that the business is disclosing the personal information to the service provider or contractor only for the limited and specified Business Purpose(s) set forth within the contract. <del>The Business Purpose shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.</del>”</p> <p><i>Apply corresponding edits to the similar language in Section 7053(a)(1).</i></p> |
| <p>Proposed Regulations §§ 7025, 7026</p> <p>Cal. Civ. Code §§ 1798.135(b), 1798.185(a)(19)–(20)</p>                           | <p>The statutory design plainly contemplates that it should be optional, not mandatory, for businesses to honor global opt-out preference signals.</p>   | <p><i>Amend language in the Proposed Regulations implying that processing the opt-out preference signal is mandatory, including in §§ 7025(b), 7025(c)(1),(3)–(4), 7026(a), etc.</i></p> <p><i>Further, include technical specifications for opt-out preference signals under §§ 7025 and 7026, as discussed in greater detail in our prior comments.</i></p>   |

---

**From:** David LeDuc [REDACTED]  
**Sent:** Monday, November 21, 2022 7:59 AM  
**To:** Regulations  
**Subject:** CPPA Public Comment  
**Attachments:** PastedGraphic-2.tiff; NAI\_comments\_Modified Proposed CPRA Regulations\_112122.docx.pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

On behalf of the Network Advertising Initiative (NAI), please find enclosed comments to the modified proposed regulations to the CPPA.

David LeDuc  
Vice President, Public Policy  
Network Advertising Initiative  
409 7th Street, NW, Suite 250  
Washington, DC 20004

P: [REDACTED] | [REDACTED]

November 21, 2022

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

Dear California Privacy Protection Agency,

On behalf of the Network Advertising Initiative (“NAI”), we appreciate the opportunity to provide comments on the proposed modified regulations under the California Privacy Rights Act (“CPRA”).

The Network Advertising Initiative (NAI) is the leading self-regulatory organization dedicated to responsible data collection and use by advertising technology companies engaged in Tailored Advertising and Ad Delivery and Reporting. For over 20 years, the NAI has promoted a robust digital advertising industry by maintaining and enforcing the highest voluntary standards for the responsible collection and use of consumer data for digital advertising. Our member companies range from large multinational corporations to small startups and represent a significant portion of the digital advertising technology ecosystem.

Thank you for considering the comments we provided during the initial comment period on the proposed regulations, and for incorporating a series of changes to address some of those recommendations. We particularly appreciate the sentiment expressed unanimously by the Board members at the meeting on October 28-29th, for the California Privacy Protection Agency (“Agency”) to be a “reasonable enforcement agency,” and the subsequent addition of language directing the Agency to consider a business’ “good faith efforts to comply with those requirements.”<sup>1</sup> We believe this should be a key principle for Agency enforcement efforts in perpetuity, and it will be particularly important if the Agency proceeds with enforcement on July 1, 2023, less than six months after the finalization of initial implementing regulations.

However, the NAI remains concerned that a series of fundamental additional modifications are necessary to bring the regulations in line with the CPRA, particularly those that we previously

---

<sup>1</sup> CA . CODE REGS. tit. 11 §7301(b).

identified regarding opt-out preference signals (“preference signals”).<sup>2</sup> We hope you will consider further updates in this area as you initiate additional regulatory proceedings.

At this time, we submit the following limited additional comments pertaining to two key sections where we believe more time and consideration are necessary before adopting the proposed modified regulations. We also respectfully request enhancements to the rulemaking process for future proceedings to ensure a greater opportunity for engagement and input by stakeholders.

### **I. § 7025: Opt-Out Preference Signals**

First, the modified proposed regulations add a new term in Sec. 7025, “pseudonymous profiles,” that is not defined by either the CPRA or proposed regulations, and they create a new requirement for businesses to extend the application of opt-out preference signals for “...any consumer profile associated with that browser or device, including pseudonymous profiles.”<sup>3</sup>

Pseudonymous identifiers are used by NAI members and across the digital advertising industry principally to avoid associating inferences for tailored advertising with specific individuals. This has long been a requirement of the NAI Code of Conduct, which differentiates between “device-identified information” and “personally-identified information,” and prohibits their merger.<sup>4</sup> It is a privacy benefit for consumers that is not required by any U.S. federal or state laws, including the CPRA. Unfortunately the new term and requirement do not provide clear direction for businesses regarding how to apply preference signals to “pseudonymous profiles.” Therefore, the NAI recommends deleting this new term and requirement until it can be considered more thoroughly and the regulations can more clearly provide guidance to businesses about what is expected.

### **II. § 7002: Restrictions on the Collection and Use of Personal Information**

Second, the NAI supports the CPRA’s emphasis on clear notice requirements, and we agree that businesses should not collect, use, and share personal information for purposes incompatible with these notices. However, Sec. 7002 of the proposed modified regulations substantially revises the restrictions, particularly in Section 7002(b), focusing on the purposes for which personal information is collected. The updated draft regulations now specify that the purposes for which personal information is collected or processed shall be consistent with the “reasonable expectations of the consumer,” which is ultimately undefined by law and is subject to a broad range of potential interpretations.

As we expressed in our initial comments to the proposed regulations, the NAI is concerned that the regulations in this area, though expansive beyond the requirements established in the

<sup>2</sup> See NAI Comments;

[https://thenai.org/wp-content/uploads/2022/08/NAI\\_Comments\\_Proposed-CPRA-Regulations.pdf](https://thenai.org/wp-content/uploads/2022/08/NAI_Comments_Proposed-CPRA-Regulations.pdf).

<sup>3</sup> CA . CODE REGS. tit. 11, § 7025(c)(1)(proposed).

<sup>4</sup> NETWORK ADVERTISING IN TATE, 2020 Code of Conduct, § II.E.2 (2020).

CPRA, remain substantially ambiguous. Unfortunately, the modified proposed regulations potentially provide less clarity, instead leaving more uncertainty for businesses about what is expected of them for a wide range of practices.

We note that this section of the proposed regulations was of substantial interest and disagreement among board members during the October 27-28, board meeting. Board member Lydia de la Torre suggested that the Agency delay any implementing regulations in this section until such time as the Agency has had a greater opportunity to discuss and refine the regulations, including the goal to align requirements as closely as possible to requirements established by other laws, noting that the Agency is not required to develop regulations on this section in the CPRA. The NAI concurs with this sentiment, and we therefore recommend that the Agency strike this section from the modified proposed regulations and revisit in future rulemakings that the Agency has committed to conducting. Such a step would facilitate greater consistency for business and consumers, particularly in the early days of CPRA implementation.

### **III. Future CPRA Rulemaking Process**

Over the last two weeks, the NAI has been actively engaging in the open stakeholder process conducted by the Colorado Department of Law (CDL), as an initial step to gain input into the rulemaking process for the Colorado Privacy Act. This interactive process has provided the opportunity for stakeholders, including businesses, civil society, and other stakeholders such as the CPPA staff, to not only submit initial written comments, but also to engage directly in civil discussion. It was particularly valuable for the NAI and other stakeholders to have the CDL pose a series of questions highlighting opportunities and challenges posed by the proposed regulations, with the goal to balance strong privacy objectives with pragmatic rules to enable more effective compliance.

This process contrasts with how the CPPA has conducted its own rulemaking process for the CPRA thus far. Notably, in the agency Board meeting on October 28-29th, there were concerns expressed among the Board about the rushed process and lack of discussion on multiple key items. Also, stakeholders were not provided with a meaningful opportunity to engage directly. Instead, public comments were invited only at the end of that meeting, after the Board had already drafted and all but committed to a motion directing the CPPA staff to modify the proposed regulations in accordance with the discussion.

The NAI recognizes that California law establishes a formal process and detailed set of requirements for drafting and approval of implementing regulations, but we do not believe these requirements should be viewed as a ceiling, but rather a floor for public engagement for regulations that will have a substantial impact on businesses across the country. Indeed, this is consistent with the law's requirement to "solicit broad public participation."<sup>5</sup> We also recognize and support the CPPA's goal to finalize this set of implementing regulations as soon as

---

<sup>5</sup> See CAL. CIV. CODE § 1798.185(a).



reasonably possible to best meet the CPRA statutory requirements for the law to become operative in January 2023, and enforcement to begin on July 1, 2023.

However, as the leading self-regulatory association for digital advertising, we engage deeply with our members and other stakeholders in an effort to interpret draft regulations, and to provide valuable input to the Agency. We therefore hope you will consider enhancing the process for future rulemakings to enable more robust participation by the NAI and other stakeholders committed to aiding industry compliance.

#### **IV. Conclusion**

The NAI recognizes and concurs with the Agency's goals to provide clear implementing regulations for the CPRA as soon as reasonably possible, and we hope you will consider these recommendations as consistent with your efforts at this time. If we can provide any additional information, or otherwise assist your office as it continues to engage in the rulemaking process, please do not hesitate to contact me at [REDACTED].

\*\*\*\*\*

Respectfully Submitted,

David LeDuc  
Vice President, Public Policy  
Network Advertising Initiative (NAI)

---

**From:** Daniella Doern [REDACTED]  
**Sent:** Monday, November 21, 2022 7:59 AM  
**To:** Regulations  
**Cc:** Lisa LeVasseur  
**Subject:** FW: CPPA Public Comment  
**Attachments:** ISL CPPA Public Comment 11-21-2022 FINAL.pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear California Privacy Protection Agency,

Please use this final version as ISL's public comment. Apologies for the internal confusion this morning.

Thank you,

**INTERNET  
SAFETY  
//LABS**

**Daniella Doern**  
Policy Advocacy Manager

**Web:** [www.internetsafetylabs.org](http://www.internetsafetylabs.org)

We've changed our name but not our mission!  
**The Me2B Alliance** is now **Internet Safety Labs**

---

**From:** Daniella Doern  
**Sent:** Monday, November 21, 2022 7:39 AM  
**To:** Regulations <regulations@cppa.ca.gov>  
**Cc:** Lisa LeVasseur [REDACTED]  
**Subject:** CPPA Public Comment

Dear California Privacy Protection Agency,

Please see the attached PDF for Internet Safety Lab's public comment.

Thank you,

**INTERNET  
SAFETY  
//LABS**

**Daniella Doern**  
Policy Advocacy Manager

**Web:** [www.internetsafetylabs.org](http://www.internetsafetylabs.org)

We've changed our name but not our mission!  
**The Me2B Alliance** is now **Internet Safety Labs**



November 21, 2022

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

**Dear California Privacy Protection Agency Staff,**

We appreciate and commend the Staff for their many positive changes in the Modified Text of the Proposed Regulations. We are particularly pleased to see the proposed changes in sections §7002; §7004; and §7051 that align with our ISL Safety Criteria and Initial Recommendations on the Text of the Proposed Regulations.<sup>1</sup>

However, we must address the proposed change in §7012 because removing the requirement to identify third parties in privacy notices is a disturbing step backwards. Based on the Agency's released Explanation of Modified Text of the Proposed Regulations, we understand that the notice requirement for businesses to identify the names of third parties that control the collection of personal information, or in the alternative, provide information about the third parties' business practices when the third party controls the collection of Personal Information was deleted to simplify implementation of the proposed regulations.

This notice requirement is not too onerous for businesses because businesses should already know (either through actual knowledge or constructive knowledge) who the third parties are and what their data practices consist of.

Requiring a Business to compile a simple list of third party names and/or third party business practices would not be a difficult task for a business to complete. Especially given that the Business will already have access to the information since the third party's name and/or business practice is relevant information that is already required by the proposed regulation's implementation of contractual requirements.

---

<sup>1</sup> In our last public comment to the Agency on the Text of the Proposed Regulations, we included our Consumer Safety Scorecard, which compared the Proposed Regulations against our ISL Safety Criteria. *For ease of access, an excerpt of the original safety score and the modified safety score after the change in §7012(e)(6) and §7012(g)(2) can be found in Figure 1 and Figure 2 on page 3.*

Businesses should easily be able to assemble a list of known third party entities, integrated into the software in any capacity, if Businesses cannot assemble this list together quickly then they have bigger structural problems to address in their software procurement process and in their data supply chain management.

GDPR already requires transparency from all data controllers by requiring data controllers to provide the identity of the controllers. In the EU, Data subjects are aware of the data controller names, purpose of collection, secondary uses of data, and if third parties have access to their information.

Moreover, both Apple and Google app store labels have moved towards greater third-party transparency, requiring the identification of third parties with whom data is shared.

The moment is here, the movement for transparency is happening. Why would the Agency step away from the notice requirement completely to simplify the implementation of the proposed regulations instead of just staying on course and delaying enforcement?

Therefore, we respectfully disagree with the proposed deletion and hope that the Agency will consider keeping the original text in §7012(e)(6) and §7012(g)(2) intact.<sup>2</sup> Consumers deserve to know who the third parties are and (at minimum the third parties' business practices) to truly be able to provide informed consent. Providing a consumer with complete and accurate notice of the third parties' names and/or business practices greatly outweighs the minimal administrative burden placed on the Business.

Sincerely,

Internet Safety Labs

---

<sup>2</sup> We do recognize that the Agency attempts to address the obligations for Third Parties that Control the Collection of Personal Information in §7012(g), but we do not believe the text of the regulation goes far enough when §7012(g)(2) is omitted.

Figure 1 – Original Score (Text of the Proposed Regulations)






| ISL CONSUMER SAFETY SCORECARD v1.0 |   |   |  |   |
|------------------------------------|---|---|--|---|
| #                                  | ISL SAFETY CRITERIA   | ISL SAFETY SCORE  | CCPA REFERENCES & RATIONALE  | RECOMMENDATIONS TO THE AGENCY   |
| <b>SAFE NOTICE PRINCIPLES</b>      |   |   |  |   |
| 2                                  | Regulation requires all B-s to provide data subjects with complete & accurate notice.   |  | §7010-7012   | Consumers deserve to know the identity of the third parties that have their personal information. This knowledge would enable consumers to act on their behalf or empower trusted third parties to act on their behalf for their best interest. Without having this knowledge consumers are forced to rely on limited government resources. |
| a                                  | All B-s must provide complete & accurate notices.                                       |  | §7010-7011<br>B-s that control the collection of personal information must provide notice at collection including comprehensive description of online & offline practices.   |   |
| b                                  | Including identification of all third-party entities that receive personal information. |  | §7012<br>Notice does not require B-s to disclose a list of all third parties. Instead, B-s are given the option to either identify third parties or provide information about the third parties' data practices within its notice. | Regulation should require B-s to list all third parties. We understand that there are situations where third parties aren't known to the B such as with the use of AdTech, which is discouraged in our ISL Safety Criteria #13 below.   |

Figure 2 – Amended Score (Modified Text of the Proposed Regulations)

|   |   |   |   |  |
|---|---|---|---|--|
| b | Including identification of all third-party entities that receive personal information. | <br> | §7012(e)(6)<br>B-s are not required to disclose a list of all third parties or provide information about the third parties' data practices within its notice. |  |
|---|---|---|---|--|

---

**From:** Michael Kans <[REDACTED]>  
**Sent:** Monday, November 21, 2022 9:28 AM  
**To:** Regulations  
**Subject:** CPPA Public Comment  
**Attachments:** California Privacy Protection Agency Comment\_Michael Kans Esq.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear sir or madam,

Please find attached my comment the California Privacy Protection Agency's (CPPA) Modified Text of Proposed Regulations as announced in the agency's Notice of Modifications to Text of Proposed Regulations. [OAL FILE NO. 2022-0628-02].

Thanks,

Michael

California Privacy Protection Agency  
 Attn: Brian Soublet  
 2101 Arena Blvd., Sacramento, CA 95834  
[regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

**Re: NOTICE OF MODIFICATIONS TO TEXT OF PROPOSED REGULATIONS AND ADDITION OF DOCUMENTS AND INFORMATION TO RULEMAKING FILE [OAL FILE NO. 2022-0628-02]**

Dear Mr. Soublet and the California Privacy Protection Agency,

I am submitting comments on the California Privacy Protection Agency's (CPPA) [Modified Text of Proposed Regulations](#) as announced in the agency's [Notice of Modifications to Text of Proposed Regulations](#). Thank you for the opportunity to comment on this most recent round of regulations to effectuate the amendments to the "California Consumer Privacy Act of 2018" (AB 375) (CCPA) made by voters via Proposition 24 (aka "California Privacy Rights Act (CPRA)).

I am an attorney<sup>1</sup> in private practice who specializes in technology law, policy, and politics with over 15 years of experience as United States (U.S.) Congressional staff and a lobbyist and lawyer. I have deep subject matter knowledge in data protection, data privacy, data security, cybersecurity, Internet of Things (IoT), U.S. government procurement, health data protection, international data flows, U.S. surveillance law, and other areas. At present, I write and publish a subscription newsletter, [The Wavelength](#), that covers technology developments in the United States, the European Union, and elsewhere. I have written extensively on the (CCPA), various bills in the California legislature to amend the CCPA, the CPRA, and many of the bills introduced in the U.S. Congress to alter U.S. privacy law.<sup>2</sup> I also consult, and, in the interest of full disclosure, I have no clients with interests in this rulemaking.

I would offer the following suggestions and observations to help the CPPA write regulations that will strengthen privacy rights in California, a primary goal of both the CCPA and CPRA.

---

<sup>1</sup> Member of the Bar Associations in the District of Columbia and Maryland.

<sup>2</sup> A sample of articles includes: *Privacy Bill Revived and Revised in Washington State*, Michael Kans Blog (February 4, 2020), <https://michaelkans.blog/2020/02/04/privacy-bill-revived-and-revised-in-washington-state/>; *Third Set of Draft CCPA Regulations Released For Comment* Michael Kans Blog (March 20, 2020), <https://michaelkans.blog/2020/03/20/third-set-of-draft-ccpa-regulations-released-for-comment/>; *CCPA 2.0 Backers Submit Ballot Initiative for November Election*, Michael Kans Blog (May 9, 2020), <https://michaelkans.blog/2020/05/09/ccpa-2-0-backers-submit-ballot-initiative-for-november-election/>; *CPRA Analyzed*, Michael Kans Blog (August 28, 2020), <https://michaelkans.blog/2020/08/28/cpra-analyzed/>; *CPRA From Another View*, Michael Kans Blog (September 2, 2020), <https://michaelkans.blog/2020/09/02/cpra-from-another-view/>; *Two State Privacy Bills Advance*, The Wavelength (March 9, 2021), <https://thewavelength.substack.com/p/two-state-privacy-bills-advance>; *Washington State Privacy Act Advances*, The Wavelength (April 6, 2021), <https://thewavelength.substack.com/p/washington-state-privacy-act-advances>; *Utah's Privacy Bill*, The Wavelength (March 8, 2022), <https://thewavelength.substack.com/p/utahs-privacy-bill>; *Three of the Four Top Privacy Stakeholders Float A Compromise Discussion Draft*, The Wavelength (June 6, 2022), <https://the-wavelength.ghost.io/three-of-the-four-top-privacy-stakeholders-float-a-muddled-discussion-draft/>; *California Proposes New Regulations To Implement CCPA Rewrite*, The Wavelength (June 9, 2022), <https://the-wavelength.ghost.io/california-proposes-new-regulations-to-implement-ccpa-rewrite/>; *California Enacts New Privacy Regime For Children Aligned With Britain's*, The Wavelength (September 15, 2022), <https://the-wavelength.ghost.io/california-enacts-new-privacy-regime-for-children-aligned-with-britains/>; and *ADPPA vs. CPRA*, The Wavelength (September 29, 2022), <https://the-wavelength.ghost.io/adppa-vs-cpra/>.

Subsection (a) of “§ 7002. Restrictions on the Collection and Use of Personal Information” contains provisions the CPPA may not have the statutory authority to promulgate. To wit, Civil Code 1798.100(c) provides in relevant part:

A business’s collection, use, retention, and sharing of a consumer’s personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed...

And so, § 7002(a)’s first sentence tracks with this statutory provision. The potential problem comes in the next line when the CPPA seeks to construe what is “reasonably necessary and proportionate” in Civil Code section 1798.100(c) and asserts that to meet this standard the “business’s collection, use, retention, and/or sharing must be consistent with what an average consumer would expect when the personal information was collected.” It is the use of the “average consumer” standard that may be outside the CPPA’s remit. The CCPA uses an “average consumer” standard in a few places, notably in Civil Code section 1798.121 which states:

A consumer shall have the right, at any time, to direct a business that collects sensitive personal information about the consumer to limit its use of the consumer’s sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services, to perform the services...

That the CCPA as amended via ballot uses “average consumer” in some places and not others suggest this standard was not to be used for determining reasonably necessary and proportionate for the collection and use of personal information. While an “average consumer” standard has its merits in terms of being easily defined and easily administered, the fact remains that this standard does not have a basis in the relevant section of the CCPA. Moreover, such a standard is apt to permit personal information collection, usage, and disclosure beyond what “reasonably necessary and proportionate” would. Using a reasonably necessary and proportionate standard would convey to all players in the data ecosystem that the minimum amount of personal information needed to provide a service or product is the target they need to meet and not the more expansive “average consumer” standard.

Moreover, it should also be noted that using an average consumer standard can result in a moving target for businesses as the expectations of the average consumer change over time. It is conceivable that the average consumer comes to see increasingly egregious data collection and processing practices as reasonably necessary and proportionate. As matters stand, according to polling data, “that roughly six-in-ten U.S. adults say they do not think it is possible to go through daily life *without having data collected about them* by companies or the government” (emphasis in the original.)<sup>3</sup> Thus this reason also lends itself to arguing against the use of the average consumer threshold in § 7002.

---

<sup>3</sup> Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar and Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (November 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.



§ 7004(a)(3) should be expanded through a provision barring businesses from offering two options, say for the selling of sharing personal information, with the choice that would permit the business to sell or share being the default. One frequently encounters this choice architecture online where a website is seeking one's consent to use cookies and the choice that would allow the business to do so is already chosen, leading a distracted or unfocused person to click on the default choice. Regulators have documented evidence that use of dark patterns in this manner often affects user behavior in ways that can be harmful to them.<sup>4</sup> This practice should be barred so that Californians will be able to choose freely when presented choices per the CCPA.

§ 7011(e)(1)(B) is one of the instances in the draft regulations where the agency references "categories of sources" of personal information businesses will have a responsibility to share with consumers. The CCPA is clear on what categories of personal information and sensitive personal information are but is silent on "categories of sources." However, the regulations lack guidance on what the categories of sources should be, leaving the matter to businesses to decide how to categorize and convey to consumers the sources from which personal information, and in some cases, sensitive personal information, are obtained. The CCPA should give consideration to writing a new subsection that would provide parameters for businesses to meet in divulging categories of sources, or at the least provide illustrative examples. This is an issue throughout the draft regulations wherever "categories of sources" is used.

A similar issue is apparent in § 7011(e)(1)(C) with "commercial purposes." As with "categories of sources," this term is not defined in the CCPA and not construed in the regulations but used in many places. Presumably, most purposes that are not illegal and not "business purposes" would be considered commercial purposes. The agency might give thought to defining the term as a way to fill a gap in the CCPA or to providing some examples of commercial purposes so businesses will understand how and what they need to be telling consumers.

A crucial caveat needs to be added to §7011(e)(2)(D) and (E), specifically that consumers may opt out of the sale or sharing of personal information and sensitive personal information at any time. Otherwise, businesses may omit this key part of the right, and only those Californians who have read the law and regulations will know this right can be exercised at any time.

In § 7012(c)(3), I have misgivings about the requirements for mobile applications regarding the Notice at Collection. Unlike the requirements for online collection that mandates a link on webpages, mobile applications would be permitted to "provide a link to the notice on the mobile application's download page and within the application, such as through the

---

<sup>4</sup> Competition and Markets Authority, *Online Choice Architecture: How digital design can harm competition and consumers*, (April 2022), Page 17, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/1066524/Online\\_choice\\_architecture\\_discussion\\_paper.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1066524/Online_choice_architecture_discussion_paper.pdf); Federal Trade Commission, *Bringing Dark Patterns to Light*, (September 2022), [https://www.ftc.gov/system/files/ftc\\_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf).

application's settings menu." Hence, it is likely for mobile applications that links to the Notice at Collection will be placed on the download page and in the settings menu, two of the least conspicuous sites to notify users. It would be more effective to have the Notice at Collection provided to users when the application has launched and users may interact it with it.

§ 7013 would permit businesses to either post a "Do Not Sell or Share My Personal Information" link giving immediate effect to a consumer's choice or "to a webpage where the consumer can learn about and make that choice." This is antithetical to symmetry principles in § 7004 because it is likely many businesses will opt for the two-step process in the hopes the extra step will dissuade users or the consumer will not opt out based on what they read on the second page. It would be more empowering to consumers if businesses were required to post a "Do Not Sell or Share My Personal Information" link and an additional link "to a webpage where the consumer can learn about and make that choice." Hence, consumers would be in a position to immediately opt out of the sale or sharing of personal information or learn more should they choose. Giving businesses a choice will result in a number taking the opportunity to place an extra step in the process.

Much the same issue is present in § 7014 as in § 7013 regarding giving businesses the option of including an extra step in providing consumers a "Limit the Use of My Sensitive Personal Information" link. As with the "Do Not Sell or Share My Personal Information" link, businesses would again have the choice to let consumers immediately effectuate their preference by clicking on the link or to "lead the consumer to a webpage where the consumer can learn about and make that choice." This again adds steps. Again, I suggest that businesses be allowed to just post "Limit the Use of My Sensitive Personal Information" link or this link and another that leads people to more information.

§ 7014(f) would be improved with greater specificity about how businesses should describe the right to limit use and disclosure in its Notice of Right to Limit. Otherwise, the CCPA and consumers may find great variation across these notices and perhaps obfuscation designed to confuse consumers.

Moreover, Civil Code section 1798.121(b) bars the use or disclosure of sensitive personal information after a consumer has exercised her right to limit unless she subsequently consents. The statute and regulations are silent on how frequently a business may ask a consumer for consent to essentially reverse his decision to opt to limit use and disclosure. This seems like a gap the agency should address with guidance if not new regulations that would prevent the foreseeable situation where some online businesses or mobile applications would constantly ask those who have opted to limit the use and disclosure of sensitive personal information to reverse their decisions.

The Alternative Opt-Out Link regulations in § 7015 need revision to make clearer to consumers what the link would do. As written, businesses could give "a single, clearly-labeled link that allows consumers to easily exercise both their right to opt-out of sale/sharing and right to limit, instead of posting the two separate "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links." However, if businesses post a link labeled "Alternative Opt-Out," many people may not understand what this choice entails and so may not click on the link which provides an explanation. It would be

more effective to require a short description of the “Alternate Opt-Out” option as part of the link that makes clear this option allows consumers to both stop the selling and sharing of personal information and limiting the use and disclosure of sensitive personal information.

The requirement in § 7016(d) that businesses, among other information, must furnish a “good-faith estimate of the value of the consumer’s data” and “[a] description of the method(s) the business used to calculate the value of the consumer’s data” may pose difficulties. Some businesses may opt for overly confusing or complex information so as to ward off scrutiny by the CCPA and consumers. The agency should consider adding what might be considered a requirement that these portions of the financial incentives disclosures meet the requirements of § 7003(a) and § 7003(b) (i.e. mathematical language that is “easy to read and understandable to consumers” and uses “plain, straightforward language and avoid technical or legal jargon.”) Such a requirement would make clear the financial proposition before consumers in a financial incentive program.

Regarding methods for submitting requests to delete, correct, and know in § 7020, in subsections (a) and (b), the agency might give thought about providing a bit more detail on what constitutes a “direct relationship.” This concern is raised because some businesses may opt to liberally construe what is a “direct relationship” (e.g. a media site claiming visits constitute a direct relationship as opposed to something more substantial like a subscription or purchases.) The motivation for broadly construing this term would be to limit their responsibility in providing means for consumers to contact them to exercise their rights. Not only might this save such a business administrative trouble but it may also function as a means of making it harder to exercise rights that could decrease the value of data businesses are collecting, processing, and sharing.

In the same vein, § 7020(d)’s bifurcated process for exercising one’s right to delete invites mischief from some businesses even with the caveat that they observe § 7004. A better model would be having the online process ask the person twice if they want to delete on the same webpage. Moreover, the CCPA does not call for a two-step process in exercising this right.

§ 7022(a) would be improved with language mandating that in denials of a request to delete businesses explain generally verification requirements for requests to delete so that consumers will better understand the type of information they need to furnish.

The CCPA might consider expanding the scope of the personal information service providers and contractors must delete in § 7022(b)(2). Civil Code section 1798.105(c)(3) provides:

A service provider or contractor shall cooperate with the business in responding to a verifiable consumer request, and at the direction of the business, ***shall delete...personal information about the consumer collected, used, processed, or retained by the service provider or the contractor*** (emphasis added.)

While Civil Code section 1798.105(a) provides that businesses need only delete personal information they collected from a consumer, meaning personal information obtained from other means need not be deleted, subsection (c)(3) requires the services providers and contractors of businesses to respond to requests to delete “personal information about the

consumer collected, used, processed, or retained by the service provider or the contractor.” Thus, the plain language of the CCPA would allow the CPPA to require service providers and contractors to delete all personal information of a consumer if she makes that request regardless of where it was acquired.

Elsewhere in § 7022, the agency should expand on what constitutes “impossibility” or “disproportionate effort.” As with other undefined or ambiguous terms, these will undoubtedly be read in ways that do not accrue to the benefit of consumers.

The CPPA should add a timeframe under which a business, service provider, or contractor should delete personal information on archived or backup systems per the verified request of a consumer in § 7022(d). Recognizing that it is impractical to set a deadline of 45 days, a deadline of three to six months may be appropriate in giving businesses, service providers, contractors, and third parties sufficient time to comply with requests while also ensuring requests will be completed in a specified timeframe. The same concern is raised by similar language in other sections of the regulations such as § 7023(c), and I suggest a similar change in those places.

In § 7022(g), the CPPA should consider requiring businesses to include in their denials of request to delete information about and an offer for the consumer to opt out of the sale and sharing of their personal information. If the agency added this requirement, then there would be question about the timeframe within which this offer must be made. As matters stand, the provision could be read as permitting a business to wait in making the offer to the requester to opt of the selling and sharing of personal information.

In § 7022(h), the agency should add a requirement that this subsection must comport with § 7004 on dark patterns, in particular, as there is the potential for the some businesses to try to use deceptive means to get consumers to choose to delete less personal information. Moreover, the choice put to consumers should be clear and easily understandable regarding the categories of personal information they can have deleted instead of all their personal information.

The revised regulations should be changed back to they were originally written with respect to § 7023(i) in that businesses should be required to “provide the consumer with the name of the source from which the business received the alleged inaccurate information.” Otherwise, a consumer seeking the source of inaccurate information would be in the Kafkaesque situation of being unable to trace the origin of wrong information. Businesses should be required to make a good faith effort to share what they know about the source of inaccurate information short of revealing confidential information or trade secrets, of course.

§ 7024(k)(3) does not match the CCPA in terms of the disclosure a business must make to a consumer under a request to know. Civil Code section 1798.110(c)(3) requires that a business that collects personal information about consumers must disclose, among other information, “[t]he business or commercial purpose for collecting, selling, or sharing personal information.” However, § 7024(k)(3) merely requires the disclosure of “[t]he business or commercial purpose for which it collected or sold the personal information.” In order to

ensure that the regulations meet the CCPA the business and commercial purposes for sharing personal information must be added to § 7024(k)(3).

In the subsection on Opt-Out Preference Signals, I have concerns that the language in subsection § 7025(b)(1) directing businesses to accept these signals if they are “in a format commonly used and recognized by businesses.” This provision could allow some businesses to reject some opt-out preference signals on the grounds the business does not consider them commonly used. It would be well if the CPPA added a provision to the regulations directing businesses to a list the agency would maintain on the signals it deems commonly used.

§ 7025(c)(5) is not clearly written and needs revision as it is not intelligible. Perhaps the agency intended to write regulations to address situations like the illustrative example in (c)(7)(B) in that “Business O may inform Noelle that her opt-out preference signal differs from her current privacy settings and provide her with an opportunity to consent to the sale or sharing of her personal information, but it must process the request to opt-out of sale/sharing unless Noelle instructs otherwise.” If the agency means to bar businesses from interpreting a lack of answer or response to a warning that a consumer’s opt-out preference signal is at odds with a previous arrangement to sell or share their personal information, then this section should be rewritten along the lines of:

Where the consumer is known to the business [and permits the sale or sharing of personal information], the business shall not interpret the absence of [a response to notification that the opt-out preference signal differs from the previously granted consent to sell or share personal information] after the consumer sent an opt-out preference signal as consent to opt-in to the sale or sharing of personal information (with bracketed language being additions to the regulations.)

In order to ensure that consumers are fully informed and knowledgeable about how their personal information is used, § 7025(c)(6) should revert to its previous form in requiring businesses to confirm a consumer has opted out. If there is not some confirmation, then a consumer may think he has opted out of the selling or sharing of his personal information or has limited the use and disclosure of sensitive personal information but has not. Therefore the consumer may continue using a website, product, or service wrongly thinking his intentions have been honored. This would be contrary to one of the CCPA’s goals: that consumers have “the information necessary to exercise meaningful control over businesses’ use of their personal information.”

§ 7025(d) should be amended to require businesses to maintain records of which consumers have opted out and that any such records can only be used for this purpose. Such a change would provide evidence in the event of an enforcement action that would show whether a business is complying with the CCPA and its regulations.

§ 7025(e) appears contrary to the CCPA. It gives me no pleasure to disagree with the CPPA’s interpretation of Civil Code section 1798.135(b)(1) and (3), but my read of the statute is contrary to the agency’s drafted regulations and the explanation provided in the “Initial Statement of Reasons.” 1798.135(b)(3) clearly establishes that “[a] business that complies with subdivision (a) is not required to comply with subdivision (b).” Of course, subdivision (a)

establishes the requirements of the “Do Not Sell or share My Personal Information” and the “Limit the Use of My Sensitive Personal Information” links along with “a single, clearly labeled link” in lieu of having both the aforementioned links.

Subdivision (b)(1) of Civil Code section 1798.135 states “[a] business shall not be required to comply with subdivision (a) if the business allows consumers to opt out of the sale or sharing of their personal information and to limit the use of their sensitive personal information through an opt-out preference signal sent with the consumer’s consent by a platform, technology...” If this were the extent of requirements on the parameters of links and opt-out preference signals, weight would be given to the CPPA’s interpretation in § 7025(e) that “[e]ven if the business posts the above-referenced links, the business must still process opt-out preference signals.” However, as noted above, 1798.135(b)(3) clearly establishes that “[a] business that complies with subdivision (a) is not required to comply with subdivision (b).” Consequently, requiring businesses that opt for subdivision (a) to also honor subdivision (b) is against the will of the voters who agreed to Proposition 24. This must be removed from the regulations, for the agency will inevitably be challenged in court at the risk of losing.

In § 7025(f)(3) businesses are prohibited from displaying “a notification, pop-up, text, graphic, animation, sound, video, or any interstitial content in response to the opt-out preference signal.” And yet, § 7025(c)(6) permits a business to “display on its website “Opt-Out Preference Signal Honored” when a browser, device, or consumer using an opt-out preference signal visits the website, or display through a toggle or radio button that the consumer has opted out of the sale of their personal information.” It would appear that some clarification is needed with respect to what a “notification” is for purposes of the prohibition in (f)(3) because the feature businesses may use per (c)(6) seems very much like a notification.

§ 7026(f)(1) sets a definite 15 day deadline by which businesses must stop selling or sharing personal information which matches § 7027(g) with respect to limiting the use and disclosure of sensitive personal information. The CPPA should consider the benefits to consumers of setting definite deadlines by which businesses must comply with verified requests to delete, correct, and know. § 7021 details the timeline for business responses to and processing of requests but is silent on the timeframe within which action is required on a verified request. The agency should consider a deadline that is fair to both businesses and consumers so there is clarity about when a verified request should be completed.

Additionally, the agency should rewrite § 7027(h) to require businesses to confirm receipt of and compliance with a request to limit use and disclosure of sensitive personal information. Thus consumers can be sure that their request was processed and being honored. The proposed means by which a consumer would learn whether their request has been effectuated places the onus on the consumer. The business must inform service providers, contractors, and third parties, so additional notice to the consumer is a marginal burden at worst.

§ 7053(a)(3) should be changed to require contracts between businesses and third parties to mandate that the latter must “comply with a consumer’s request to opt-out of sale/sharing forwarded to it by a first party business.” Civil Code section 1798.100(d) makes abundantly clear in subsection (2) that contracts with third parties obligates these entities “to comply

with applicable obligations under this title and obligate those persons to provide the same level of privacy protection as is required by this title.” If third parties are not required to honor opt-out requests because their contracts with businesses may not require doing so under the regulations, then they cannot be said to be complying with the “applicable obligations” under the CCPA. Hence, § 7053(a)(3) should require that contracts between businesses and third parties so that the latter will understand clearly their legal obligations.

The CPPA should give thought to establishing what a “more stringent verification process” means with respect to the provisions in § 7060(c)(3). It seems probable and foreseeable that some businesses will read this phrase as requiring the setting of a standard so high that many requests will not be verified.

§§ 7060, 7061, and 7062 need language making clear to businesses that weaponizing the verification process as a means of defeating properly submitted consumer requests is a violation of the CCPA. At least [one study](#) has found that, at present, some businesses in California seem to be making verification as hard as possible to ward off consumer requests.<sup>5</sup> Moreover, as the agency is likely well aware of, many of the Attorney General’s case examples relate to issues with consumer requests and verification.<sup>6</sup> Should the CPPA add language emphasizing that intentional efforts to complicate their process for processing and verifying consumer requests violate the CCPA, the agency should consider adding it to the sections of the regulations on the rights to delete, correct, know, opt-out of the sale and sharing of personal information, and to limit the use and disclosure of sensitive personal information.

In the same vein, in light of the ample latitude given to businesses in verifying the identity of adults for the exercise of CCPA rights, the methods of verifying the identity of a child’s parent are much less rigorous with respect to consent to sell or share a child’s personal information. For example, § 7070(a)(2) permits businesses to rely on a phone call with a parent or a guardian to allow the personal information of a more vulnerable group of individuals to be sold or shared. In light of language on verification for adults, it is paradoxical that the methods for verifying the identities are lax for a class of individuals intended to receive higher protection under the CCPA. The agency might consider permitting adults — again, a group that would receive less protection generally — to use the same identity verification methods for themselves that they can avail themselves of for their children. The same is applicable to adults’ identity verification vis a vis the methods of identity verification in § 7070(c) for determining a parent or guardian’s identity for purposes for exercising the rights to delete, correct, and know.

Given the statute of limitations in Civil Code sections 1798.199.70 and 1798.199.75(b), the CPPA might consider extending the period that businesses must maintain records of consumer requests to match accordingly in § 7101 to more than two years.

---

<sup>5</sup> Kaveh Waddell, *California's New Privacy Rights Are Tough to Use, Consumer Reports Study Finds*, Consumer Reports (March 16, 2021), <https://www.consumerreports.org/privacy/californias-new-privacy-rights-are-tough-to-use-a1497188573/>.

<sup>6</sup> CCPA Enforcement Case Examples, California Attorney General, <https://oag.ca.gov/privacy/ccpa/enforcement>.

Even though I agree with § 7102 “Requirements for Businesses Collecting Large Amounts of Personal Information” on a policy basis, there is scant basis for these provisions in the CCPA. Of course, the Attorney General, and now the CCPA, were given wide discretion in Civil Code 1798.185(a) “adopt regulations to further the purposes of this title, including, but not limited to, the following areas,” but a higher set of requirements for the holders of large amounts of data is not evidenced anywhere else in the CCPA. Accordingly, the agency should strike these provisions.

Civil Code section 1798.185 directs the CPPA to undertake a rulemaking, which it has done in substantial part. However, the agency did not address a number of issues the amended CCPA requires. For example, Civil Code section 1798.185(a)(12) directs the Attorney General “to further define “intentionally interacts,” with the goal of maximizing consumer privacy.” However, as I probably do not need to remind the CPPA, it assumed the Attorney General’s rulemaking authority on April 21, 2022. Hence, the onus falls on the CPPA to fulfill the will of the voters of California who voted to approve Proposition 24 in part through meeting all the rulemaking requirements. And yet, a number of items the CPRA directed the CPPA to include are not in the revised regulations.

Likewise, the present regulations do not meet these other requirements in Civil Code section 1798.185:

- (12) Issuing regulations to further define “intentionally interacts,” with the goal of maximizing consumer privacy.
- (13) Issuing regulations to further define “precise geolocation,” including if the size defined is not sufficient to protect consumer privacy in sparsely populated areas or when the personal information is used for normal operational purposes, including billing.
- (14) Issuing regulations to define the term “specific pieces of information obtained from the consumer” with the goal of maximizing a consumer’s right to access relevant personal information while minimizing the delivery of information to a consumer that would not be useful to the consumer, including system log information and other technical data. For delivery of the most sensitive personal information, the regulations may require a higher standard of authentication provided that the agency shall monitor the impact of the higher standard on the right of consumers to obtain their personal information to ensure that the requirements of verification do not result in the unreasonable denial of verifiable consumer requests.
- (15) Issuing regulations requiring businesses whose processing of consumers’ personal information presents significant risk to consumers’ privacy or security, to:
  - Perform a cybersecurity audit on an annual basis, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent. The factors to be considered in determining when processing may result in significant risk to the security of personal information shall include the size and complexity of the business and the nature and scope of processing activities.
  - Submit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and



identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public. Nothing in this section shall require a business to divulge trade secrets.

- (17) Issuing regulations to further define a “law enforcement agency-approved investigation” for purposes of the exception in paragraph (2) of subdivision (a) of Section 1798.145.

I would urge the CPPA to promulgate the regulations necessary to effectuate these sections of the CCPA.

Please do not hesitate to contact me should you require additional information or clarification.

Regards,

Michael Kans

---

**From:** franksalinger [REDACTED]  
**Sent:** Monday, November 21, 2022 9:24 AM  
**To:** Regulations  
**Subject:** CPPA Public Comment  
**Attachments:** CardCoalitionCPPAFiled112122.pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: franksalinger [REDACTED]

Attached are the comments of the Card Coalition in response to the Notice of Proposed Rulemaking published on November 3, 2022 to further modify proposed regulations implementing the Consumer Privacy Rights Act of 2020. Thank you for your consideration.

**Frank M. Salinger**  
General Counsel  
Card Coalition  
[REDACTED]  
[www.cardcoalition.org](http://www.cardcoalition.org)

Notice: If received in error, please delete and notify sender. Sender does not waive confidentiality or privilege and use or transmittal of any content is prohibited.



November 21, 2022

California Privacy Protection Agency  
ATTN: Brian Soublet, Esquire  
2101 Arena Boulevard  
Sacramento, CA 95834  
Filed via email at [regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

Re: CPPA Public Comment

Dear Mr. Soublet:

The Card Coalition respectfully submits these comments in response to the Notice of Proposed Rulemaking published on November 3, 2022 to further modify proposed regulations implementing the Consumer Privacy Rights Act of 2020 (CPRA).

Our concerns and recommendations were noted in our August 23, 2022 comment letter and we urge you to further amend the draft.

### **Statement of Interest & Policy Concerns**

The Card Coalition consists of major national card issuers and related companies interested in state legislative, executive, and regulatory activities affecting the credit card industry and consumers. We are the only national organization devoted solely to the payment card industry and related legislative and regulatory activities in all 50 states.<sup>1</sup>

Few industries are as keenly aware of the need to protect our customers' privacy, and we appreciate the opportunity to participate in this important rulemaking.

We are concerned about practical compliance issues which arise when your agency

---

<sup>1</sup> The Card Coalition consists of major national card issuers and related companies with an interest in state legislative, executive, and regulatory activities affecting the credit card industry and consumers. We are the only national organization devoted solely to the credit card industry and related legislative and regulatory activities in all 50 states. To learn more about the Card Coalition and our members, please visit [www.cardcoalition.org](http://www.cardcoalition.org).

promulgates requirements unique to California without demonstrating privacy challenges that are, in some manner, unique to California. Enhancing consumer privacy protections is a global, transnational, issue and we believe individual states should move cautiously and allow regulated institutions maximum flexibility to respond to ever-evolving challenges.

We continue to note that, in many instances, the proposed regulations exceed what is required by the underlying statute. This comment letter references provisions we believe should be amended to follow the underlying statute.

While passage of the CCPA was a significant event and a number of states carefully considered enacting comprehensive privacy laws, only five states have done so—most of them less burdensome to business.<sup>2</sup>

Adding extra-statutory requirements adds needless compliance challenges with little apparent benefit to California consumers. We urge you to adopt our suggested changes.

### **Specific Areas of Concern**

#### ***a. Employee and B2B Data***

In only 41 days, the CPRA will apply to employee personal information and personal information belonging to an employee or other individual associated with another legal entity involved in a commercial transaction with a business (e.g., B2B contact details).

Applying the CPRA and its regulations to employee and B2B data will create unintended consequences and compliance problems that cannot be easily solved without further guidance and clarity.

Neither your agency nor the California Attorney General has provided businesses with any guidance regarding compliance concerning such data.

While there may be some circumstances wherein applying the law to employee or B2B data operates the same or similarly to consumer data, in other circumstances, the consumer-oriented nature of the law and its regulations makes applying the law to non-consumer data impracticable, unreasonable, or impossible.

---

<sup>2</sup> California, Colorado, Connecticut, Utah, and Virginia.

*We recommend the CPPA issue guidance providing more clarity regarding CCPA obligations concerning employee and B2B data.*

***(b) Section 7012(f) and notice at collection online.***

Section 7012(f) requires a business that collects personal information online to provide the notice at collection by providing a “link that takes the consumer directly to the specific section of the business’s privacy policy that contains the information required in subsection (e)(1) through (6).”

The section continues by stating that directing the consumer to the beginning of the privacy policy or to any other section without the required information will not satisfy the notice at collection requirement. We believe this requirement is overly prescriptive and impractical to put in place.

The notice at collection must contain a link to the privacy policy. Additionally, the notice at collection is more tailored to the products or services requested by the consumer. Should every notice at collection have different links to different sections of the privacy policy?

Further, due to the existing requirements under the CCPA, many companies have structured their privacy policies so that the information required by sections (e)(1) through (6) are part and parcel of the policy itself rather than segregated in a specific California section. In such a case it makes sense to link to the Privacy Policy as a whole.

*We continue to recommend this requirement be scrapped.*

***(c) Sections 7022(b) and (d) and archived or backup systems.***

Section 7022(b)(1) requires businesses to delete a consumer’s personal information from its existing systems except “archived or back-up systems,” seemingly indicating that requests to delete do not trigger a requirement to delete personal information on archived or back-up systems.

To the contrary, Section 7022(d) states that a business that stores any personal information on archived or back-up systems “may delay compliance with the

consumer's request" until the archived or back-up system is "restored to an active system or is next accessed or used for a sale, disclosure, or commercial purpose."

For clarification, is the proposed Regulation saying that a business is never required to delete personal information stored on archived or back-up systems (as long as it stays on such archived or back-up systems), or a business has a requirement to delete personal information on archived or stored systems; however, that requirements isn't triggered unless, or until, a business activates that system or accesses, sells, discloses, or uses such data for a commercial purpose?

Additionally, does the term "access" include *de minimus*, temporary, or transient access for maintenance, information security, fraud, system improvement, and other purposes that do not require length or permanent access nor use or disclosure of personal information outside of the limited purposes mentioned?

*We continue urge the CPPA further clarify these issues.*

***(d) Section 7026(f)(2) and downstream notification of consumer opt-out requests to all third parties.***

Section 7026(f)(2) requires a business to notify all third parties to whom the business has sold or shared a consumer's personal information of a consumer's request to opt-out of sale/sharing and to forward the consumer's opt-out request to "any other person with whom the person has disclosed or shared the personal information."

Both requirements go beyond the requirements of the statute and would be technically challenging at the device level (whether in connection with a one-off device interaction or in response to a global privacy control).

Furthermore, the requirement to forward a consumer's request to any person with whom the person has disclosed or shared the information fails to take into consideration lawful disclosures to service providers, contractors, law enforcement, government agencies, or disclosures to other businesses or individuals pursuant to an explicit request or direction from the consumers to make the disclosure.

*We believe these requirements should be dropped as, along with lacking statutory authority, are operationally difficult or likely impossible due to technological and practical limitations.*

***(e) Section 7027 and use of sensitive personal information.***

In a number of sections, the Regulations contravene and narrow the scope of the statutory language, effectively disregarding Section 1798.121(a)-(b), which permit a business to use a consumer's sensitive personal information for uses that are "necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services," even after receipt of a consumer's request to limit.

While the Regulations attempt to define permissible uses of Sensitive Personal Information in Section 7027(l), the seven use cases listed most certainly do not encompass all those uses of Sensitive Personal Information that may be "necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services."

The impact of this overreach by the Regulations has significant adverse effect. As an example, in Section 7014(h), the Regulations purport to impose a springing consent requirement with respect to any use, outside the seven limited uses defined by Section 7027(l), of Sensitive Personal Information collected at a time when a business did not have a notice of right to limit posted.

As a notice of right to limit is not required until January 1, 2023, any personal information collected prior to January 1, 2023, absent consumer consent, may not be used for any purpose other than one of the seven purposes defined by Section 7027(l).

Similarly, in Section 7027(g)(1), the Regulations require that, upon receipt of a request to limit, a business must cease to use and disclose Sensitive Personal Information for any purpose other than the 7 purposes listed in Section 7027(l); a restriction that conflicts with the language in 7027(a) and in 1798.121(a)-(b) that allows uses that are "necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services."

These inconsistencies are problematic for constructing a compliance program. The above notwithstanding, the seven use cases identified in 7027(l) fail to contemplate a use of Sensitive Personal Information to comply with a legal or regulatory obligation or otherwise address any use case that relates to uses of employee information.

*Again, we urge the CCPA to conform the proposed regulations with the underlying statute.*

***(f) Section 7051(a)(2) and Section 7053 and business purpose disclosures in service provider/contractor/third party contracts.***

Section 7051(a)(2) requires businesses identify, in each service provider or contractor agreement, the specific business purpose for which personal information is disclosed, which goes beyond the statute's obligations and beyond the contractual remediation that businesses undertook in complying with the CCPA. The draft regulations would require an impractical amount of additional contract remediation to update executed contracts with this information.

*Reiterating the position we stated in our previous comment, we continue to note Section 7053 of the draft already requires the same information for third party agreements, which goes beyond the statute's requirements and is an impractical task.*

***(g) Sections 7051(e) and 7053(e) and due diligence.***

Section 7051(e) and Section 7053(e) states that “[w]hether a business conducts due diligence of its” service providers, contractors, or third parties “factors into whether the business has reason to believe” the service provider, contractor, or third party is using personal information in violation of the CCPA/CPRA.

Furthermore, both provisions cite an example where a business that never enforces the terms of its contract nor exercises its rights to audit or test might not be able to rely on the defense that it did not have reason to believe that the service provider, contractor, or third party intended to use the personal information in violation of the CCPA. These provisions go beyond the statute and shifts service provider, contractor, and third party liability to the business.

Moreover, the provisions do not discuss what level of due diligence is required to prevent this shifting of liability.

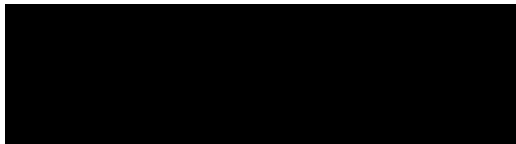
*Again, we suggest striking these provisions or amending and clarifying them such that businesses know what level of due diligence is required to prevent the shifting liability.*



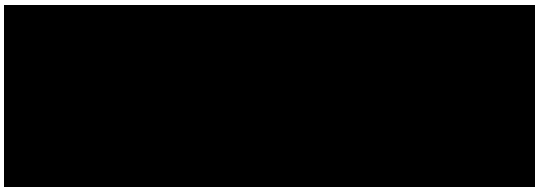
\*

The Card Coalition appreciates the opportunity to share our views on and would be pleased to discuss our specific concerns outlined above. Thank you for your consideration.

Respectfully submitted,



Toni A. Bellissimo  
Executive Director



Frank M. Salinger  
General Counsel



---

**From:** Shapiro, Tracy <[REDACTED]>  
**Sent:** Monday, November 21, 2022 11:43 AM  
**To:** Regulations  
**Cc:** Holman, Eddie  
**Subject:** CCPA Public Comment  
**Attachments:** WSGR Response to Invitation for Comments on the Modifications to the Proposed Rulemaking Under the California Privacy Rights Act of 2020.pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear Board Members and Staff of the California Privacy Protection Agency:

Attached please find our comment on the proposed rulemaking under the California Privacy Rights Act of 2020.

Sincerely,

Tracy Shapiro



Tracy Shapiro | Partner, Privacy & Cybersecurity | Wilson Sonsini Goodrich & Rosati  
One Market Street | San Francisco, CA 94105 | O: [REDACTED] | [REDACTED]

This email and any attachments thereto may contain private, confidential, and privileged material for the sole use of the intended recipient. Any review, copying, or distribution of this email (or any attachments thereto) by others is strictly prohibited. If you are not the intended recipient, please contact the sender immediately and permanently delete the original and any copies of this email and any attachments thereto.



Wilson Sonsini Goodrich & Rosati  
Professional Corporation  
One Market Plaza  
Spear Tower, Suite 3300  
San Francisco, California 94105-1126



TRACY R. SHAPIRO

Internet: [REDACTED]

Direct dial: [REDACTED]

EDDIE HOLMAN

Internet: [REDACTED]

Direct dial: [REDACTED]

November 21, 2022

California Privacy Protection Agency  
Attn: Brian Soublert  
2101 Arena Blvd.  
Sacramento, CA 95834  
[regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

**Re: Invitation for Comments on the Modifications to the Proposed Rulemaking Under the California Privacy Rights Act of 2020**

Dear Board Members and Staff of the California Privacy Protection Agency:

Wilson Sonsini Goodrich & Rosati appreciates the opportunity to submit these comments in response to the California Privacy Protection Agency's ("CPPA" or "Agency") invitation for comments on the modifications to the text of the proposed regulations implementing the California Privacy Rights Act of 2020 ("CPRA"), Cal. Code Regs. tit. 11, §§ 7000-7304 ("Modified Proposed Regulations"). We submit these comments on behalf of certain of our clients, including companies in the digital advertising ecosystem and companies that provide security and fraud prevention services, though to be clear, these comments do not necessarily reflect the views of all of our clients. These companies appreciate the importance of consumer privacy and data protection, and we submit these comments with the aim of encouraging the Agency to issue regulations that will protect the privacy of consumers in a manner that is effective, practical, and allows companies to continue to provide consumers with valuable services.

- 1. The Agency should clarify that the exception for service providers and contractors to "use" personal information to "prevent, detect, or investigate data security incidents or protect against malicious, deceptive, fraudulent or illegal activity" in Section 7050(a)(4) of the Modified Proposed Regulations includes the ability to "combine" personal information for those purposes.**

Section 1798.185(a)(10) of the CPRA tasks the Agency with further defining: (1) the business purposes for which businesses, service providers, and contractors may "use" consumers' personal information consistent with consumers' expectations; and (2) the business purposes for which service providers and contractors may "combine" consumers' personal information

CCPA Board Members and Staff  
November 21, 2022  
Page 2

obtained from different sources. Furthermore, Section 7051(a)(5) of the Modified Proposed Regulations requires that a service provider or contractor “be prohibited from combining or updating personal information that it Collected pursuant to the written contract with the business with personal information that it received from another source or Collected from its own interaction with the consumer, *unless expressly permitted by the CCPA or these regulations*” (emphasis added). Thus, it is important for the regulations to spell out when it is expressly permissible for service providers and contractors to combine or update personal information Collected pursuant to a written contract with a business. While Section 7050(a) of the Modified Proposed Regulations enumerates certain exceptions for when a service provider or contractor may “retain, use, or disclose” personal information, the Modified Proposed Regulations remain silent on the express circumstances in which service providers and contractors may “combine” personal information.

The Agency should make clear that service providers and contractors may “combine” personal information for security and fraud prevention purposes. Agency Staff already seems to hold this view: in the October CCPA Board meeting, Lisa Kim, a Deputy Attorney General of the California Department of Justice, expressed a view that “combining” is a type of “use.”<sup>1</sup> For example, she used the verb “combine” to denote the verb “use” in the Modified Proposed Regulations, stating: “we clarified where a service provider or contractor can combine personal information even when it’s not explicitly addressed in the contract, and that is notated in 7050(a)(3). . . . And again with regard to 7050(a)(4), as it relates to data security, fraud, and illegal activity.”

To codify this clarity offered by Agency Staff, the CCPA could:

- Revise Section 7050(a) to read (addition underlined): “A service provider or contractor shall not retain, use, combine, or disclose personal information Collected pursuant to its written contract with the business except: . . .”; or
- Alternatively, revise Section 7050(a)(4) to read (addition underlined): “To prevent, detect, or investigate data security incidents or protect against malicious, deceptive, fraudulent, or illegal activity, including combining and updating personal information Collected pursuant to the service provider’s or contractor’s written contract with the business as reasonably necessary and proportionate to achieve this Business Purpose, even if this Business Purpose is not specified in the written contract required by the CCPA and these regulations.”

There are many compelling reasons why service providers and contractors should be expressly permitted to combine personal information for security and fraud prevention purposes. In our clients’ experience, service providers that process personal information for security and fraud prevention purposes often need to combine personal information from multiple sources to

---

<sup>1</sup> CCPA October Board Meeting, 2:45:50, <https://youtu.be/D5uFuyOi3gE?t=9950>.

provide effective security and fraud prevention services. Combining personal information from multiple sources may, for example, enable service providers and contractors to better identify and remediate malicious activity affecting multiple businesses.

**2. The Agency should clarify that (1) ad measurement and attribution are permissible business purposes and (2) ad measurement and attribution providers can combine personal information for ad measurement and attribution purposes.**

First, the Agency should clarify that ad measurement and attribution do not constitute cross-context behavioral advertising and therefore are within the scope of permissible advertising and marketing services under CPRA Section 1798.140(e)(6) that qualify as “business purposes.” Consequently, entities that provide ad measurement and attribution services on behalf of businesses should be able to act as service providers under the CPRA.

Section 7050(b) of the Modified Proposed Regulations is currently ambiguous on this point. In the advertising industry, publishers that display online ads are often paid not by the number of the ads shown, but by the actions that consumers have taken after seeing the ad, such as purchasing a product, installing an app, or subscribing to a newsletter, i.e., “conversions.” Measuring whether the display of a particular ad resulted in a conversion is necessarily done after the ad is selected and shown to a consumer. Relatedly, “ad attribution” is the process of determining how much credit should be given to particular ad clicks for a particular conversion. Ad measurement and attribution typically require the collection of information about a consumer’s activity across different websites and services to be accurate, for example, associating clicks on ads displayed on the websites of Businesses A and B with a purchase made in Business C’s mobile app.

CPRA Section 1798.140(k) defines cross-context behavioral advertising as “the *targeting* of advertising to a consumer based on the consumer’s personal information obtained from the consumer’s activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts” (emphasis added). As explained above, however, ad measurement and attribution play no role in the *targeting* of advertising to a consumer, but rather the determination of whether the display of an ad achieved the advertiser’s goals and, if so, how the publisher should be paid. Currently, Section 7050(b) of the Modified Proposed Regulations states that “[a] service provider or contractor cannot contract with a business to provide cross-contextual behavioral advertising” and that “[a] person who contracts with a business to provide cross-contextual behavioral advertising is a third party and not a service provider or contractor with respect to cross-contextual behavioral advertising services.” Section 7050(b)(2) further explains that an advertising agency can provide contextual advertising services as a service provider by “placing advertisements for Business T’s products on websites that post recipes and other cooking tips,” but is silent as to whether the advertising agency can use ad measurement and attribution services to determine how to appropriately compensate the websites that displayed ads for Business T’s cookware products.

Additionally, ad measurement and attribution do not constitute cross-context behavioral advertising because ad measurement and attribution are aligned with the permissive business purposes defined under CPRA Sections 1798.140(e)(1) and (e)(6). CPRA Section 1798.140(e)(1) states that “[a]uditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards” is a permissible business purpose. Auditing ad impressions to verify their count, quality, and compliance with advertising standards is precisely what ad measurement and attribution do. Moreover, ad measurement and attribution are essential components of “advertising and marketing services” described in CPRA Section 1798.140(e)(6); the entire advertising and marketing services industry depends on measurement and attribution for quality control and to direct proper payment. The CPRA expressly permits contextual advertising services, but those services would not be possible without ad measurement and ad attribution.

Second, the Agency should clarify that ad measurement and attribution providers are permitted to combine personal information for purposes of providing these services. As described above, Section 1798.185(a)(10) of the CPRA tasks the CPPA with further defining: (1) the business purposes for which businesses, service providers, and contractors may “use” consumers’ personal information consistent with consumers’ expectations; and (2) the business purposes for which service providers and contractors may “combine” consumers’ personal information obtained from different sources. Furthermore, Section 7051(a)(5) of the Modified Proposed Regulations requires that a service provider or contractor “be prohibited from combining or updating personal information that it Collected pursuant to the written contract with the business with personal information that it received from another source or Collected from its own interaction with the consumer, *unless expressly permitted by the CCPA or these regulations*” (emphasis added). Thus, it is important for the regulations to spell out when it is expressly permissible for service providers and contractors to combine or update personal information Collected pursuant to a written contract with a business. While Section 7050(a) of the Modified Proposed Regulations enumerates certain exceptions for when a service provider or contractor may “retain, use, or disclose” personal information, the Modified Proposed Regulations remain silent on the express circumstances in which service providers and contractors may “combine” personal information.

The Agency should make clear that entities that provide ad measurement and attribution services on behalf of businesses may “combine” personal information for these purposes. As described above, ad measurement and attribution partners necessarily must combine data Collected from different websites and online services in order to provide their services. Moreover, the “combining” done by ad measurement and attribution providers does not appear to be the kind of “combining” that the Agency intended to prohibit based on the examples provided in Section 7050(b) of the Modified Proposed Regulations. For example, Section 7050(b)(1) describes how a social media company, when it receives personal information from a business, cannot use that information to serve ads to specific users. This type of restriction is to prohibit combining personal information (i.e., the list of customer email addresses provided by Business S with email addresses independently Collected by the social media company as a business) in order to “target” ads to consumers. The type of combining used for ad measurement and attribution, however, is

CPPA Board Members and Staff  
November 21, 2022  
Page 5

for evaluating ad performance after serving ads has taken place, as opposed to doing so in order to serve ads.

To clarify that ad measurement and attribution are permissible business purposes and that combining personal information is permitted for these purposes, the Agency could both:

- Revise Section 7050(b) of the Modified Proposed Regulations, where the Agency distinguishes what types of activities constitute combining and are therefore prohibited. The Agency could insert another example as Section 7050(b)(3) or expand the example in Section 7050(b)(2) to explicitly state that combining data for ad measurement and attribution purposes is permitted. For example, Section 7050(b)(2) could be revised to the following (additions and corrections underlined): “Business T, a company that sells cookware, hires an advertising company as a service provider for the purpose of advertising its products. The advertising company can serve Business T by providing contextual advertising services, such as placing advertisements for Business T’s products on websites that post recipes and other cooking tips. The advertising company can also combine personal information that it Collected (pursuant to its written contract with Business T) from websites where it placed the advertisement with personal information that it collected from Business T’s website to provide advertising measurement and attribution services.”; and
  - Revise Section 7050(a) to read (addition underlined): “A service provider or contractor shall not retain, use, combine, or disclose personal information Collected pursuant to its written contract with the business except: . . .”.
- 3. For clarity and consistency with the CPRA statute, the Agency should revise Section 7052(a) of the Modified Proposed Regulations to make clear that businesses are required to enter into contracts with third parties only when the business sells or shares personal information with the third party.**

Under Section 7052(a) of the Modified Proposed Regulations, a third party that does *not* have a contract with a business that complies with the requirements set forth in 7053(a) “shall not collect, use, process, retain, sell, or share the personal information that the business made available to it.” This prohibition is potentially inconsistent with both the CPRA statute and the Modified Proposed Regulations themselves. CPRA Section 1798.100(d) and Modified Proposed Regulations Section 7053(a) require a business to enter into a contract with a third party only when the business sells or shares personal information with a third party. Section 7052(a) introduces an ambiguity – i.e., it is not entirely clear whether its prohibition is intended to apply to all third parties that lack a contract with the business from which it receives personal information, or only to third parties to which the business sold or shared personal information. We think it is reasonable (and consistent with the statute) to interpret 7050(a) as applying only to the latter for the reasons below; nevertheless, CCPA-covered entities would benefit from clarity on this point.

CPPA Board Members and Staff  
November 21, 2022  
Page 6

If the Agency did intend to expand the obligations in 7053(a) to all third parties, this obligation would impose an unreasonable and, in some cases, impossible compliance burden on businesses, third parties, and consumers. For example, if a consumer intentionally directs a business to disclose their personal information to a third party, the business has not sold or shared the personal information and thus the business and third party should not have to enter into a contract to fulfill the consumer’s direction. Similarly, a business may be compelled to make personal information available to a third party in the context of a litigation or to comply with regulatory requirements, in which case entering into a contract with the third party that contains the requirements set forth in Section 7053(a) may be impossible.

Section 7052(a) of the Modified Proposed Regulations should therefore be revised to state (corrections underlined): “A third party that does not have a contract that complies with section 7053, subsection (a), shall not collect, use, process, retain, sell, or share the personal information that the business sold to, or shared with, it.” This modification would clarify that a contract between a business and third party is required only when a business sells or shares personal information with the third party, which would bring the Modified Proposed Regulations in line with CPRA’s statutory and regulatory scheme and reduce potential confusion about the circumstances under which a business must enter into third-party contracts.

Sincerely,

WILSON SONSINI GOODRICH & ROSATI  
Professional Corporation



Tracy R. Shapiro



Eddie Holman



---

**From:** Lucy Chinkezian [REDACTED]  
**Sent:** Monday, November 21, 2022 11:54 AM  
**To:** Regulations  
**Cc:** Kyla Christoffersen Powell  
**Subject:** CPPA Public Comment  
**Attachments:** CJAC Comments CPPA Rulemaking 11-21-22.pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

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

Dear CPPA:

The Civil Justice Association of California hereby submits its comments on the CPPA's proposed regulations implementing the Consumer Privacy Rights Act of 2020.

Lucy Chinkezian  
Counsel  
Mobile [REDACTED] | [www.cjac.org](http://www.cjac.org)





November 21, 2022

***Sent via email***

California Privacy Protection Agency  
Attn: Brian Soublet  
[regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

Re: *Comments by the Civil Justice Association of California on Proposed Rulemaking Under the California Privacy Rights Act of 2020*

Dear California Privacy Protection Agency Board and Staff:

The Civil Justice Association of California (CJAC) appreciates the opportunity to provide comments on behalf of our member companies and organizations to the California Privacy Protection Agency ("Agency") proposed modifications to the regulations under the California Consumer Privacy Act (CCPA), as modified by the California Privacy Rights Act of 2020 (CPRA).

CJAC appreciates the thoughtful modifications the board has made to the proposed regulations, and understands the gravity of the task at hand in striking a balance between the interests of consumers and businesses. These comments address both the latest modifications to the rulemaking as well as the original proposed rules where CJAC's suggested modifications were not adopted. We urge the Agency to adopt our previously-requested but unaccepted changes delineated in our comments dated August 23, 2022.

**1. Enforcement Deadline**

We must once again note that the Agency has failed to adequately address or otherwise discuss the impending enforcement deadline of the regulations, except briefly as it pertains to investigations of violations, despite repeated requests from a wide array of stakeholders. The enforcement deadline should not continue to be overlooked as it has.

While Section 7301(b) gives the Agency the discretion to consider good faith compliance efforts and the delay in the statutory effective date and the regulatory requirements, this does not go far enough. Given the volume of the regulations, and the complexity of the regulatory requirements, the Agency needs to establish and across-the-board extension of the enforcement deadline of at least 12 months from the date the regulations are finalized.

At a minimum, it is critical the Agency to provide a grace period for enforcement of the rules as applied to employment records. Businesses will need time to apply the rulemaking to employment records and carry out required implementation which will be especially challenging since the opt-out and deletion rights for personal information are incompatible with business functions and other legal obligations.

Business-to-business (“B2B”) situations present additional issues and a grace period should apply to B2B relationships as well. Businesses have B2B contacts, such as external associates and vendor employees, who are employed by other organizations. Their employer should be the first stop for any CCPA request, not an entity they interact with through their employer. These contacts are not the same as a business’ actual employees. In many cases, the information businesses have on them is minimal and only as a result of an agreement with their employer for services. Businesses should not be forced to treat them as their own employees with regard to CCPA requests.

## 2. Opt-Out Preference Signals [Section 7025]

The Agency maintains that honoring global opt-out preference signals is mandatory per the California Privacy Rights Act, seemingly ignoring the plain language of the text. In fact, the agency all but dismissed this view shared by the diverse stakeholders impacted by the agency’s rulemaking during its hearing discussing the proposed modifications.

We once again urge the agency not to exceed its authority by clarifying that honoring opt-out preference signals is optional by, at a minimum, replacing “shall” with “may” at Section 7025(b) and (c)(1).

We appreciate the modification to the language in Section 7025(c)(6) from “a business should” to “a business may” display whether it has processed the opt out preference signal. During the hearing, the Board expressed its belief that this change should be temporary. We urge the Board to adopt this change permanently.

CJAC has concerns about requirements in the modified rules that will interfere with function, are technologically not feasible, or are overly burdensome:

- Requirements to honor global preference signals should not exceed the capabilities of eligible global preference signals that are available in the marketplace (e.g., if only browser extensions are eligible, the requirement 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:

**Section 7025 (b):** 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.](#)

- In the example provided in Section 7025(c)(7)(A), 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:

**Section 7025(c)(7)(A):** 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.

- We do not agree with the change to the example in Section 7025(c)(7)(B) requiring a business to wait at least 12 months before asking a user who is logged in and has opted out of the sale or sharing of her personal information to opt in. 12 months is unreasonably long.
- The proposed modified regulations still need to expressly account for statutory specifications set out for the global preference signals and eliminate provisions that conflict with the statute. For instance, the modified regulations permit signals to enable by default even though explicitly prohibited in the statute.
- Additionally, the statutory specifications mandate that the signal clearly represent a consumer's intent, yet the modified regulations do not require any disclosures or other communications to consumers to explain the parameters and limitations of the California opt-out rights.
- The modified regulations do not align with the choice architecture standards required under Section 7004. Under the proposed modifications, a business cannot impair a consumer's ability to make a choice, but a global preference mechanism can enable by default and implement a choice without any disclosures to the consumer. The regulations should be revised to be consistent with the required parameters for choice architecture.
- The regulations need to be amended to impose reasonable technical requirement on the global preference mechanisms to ensure they function as intended by the statute. For instance, the regulations do not contemplate requiring the mechanism to account for any of the necessary identifying information to determine a consumer's residency that is solely within the capability of the mechanism to discern. The signals currently on the market, allow the business to collect the following: an IP address and the type of device used. Neither data point confirms that the consumer is located in California, let alone addresses residency. These

- issues are made even more difficult by the widespread use of mobile devices (which use dynamic IP addresses) and VPNs. Without access to better location information, the business cannot determine if the California opt-out rights apply. Yet, the regulations fail to solve this by requiring the mechanism, which is in the best position to identify and send this information, to do so. For instance, browser based mechanisms could use a customer/structured field in the HTTP header that is sent to website to identify the consumer's residency. This would, in turn, be sent to websites by the browser in HTTP request. This is a technical solution to residency authentication problem that the regulations need to resolve, both in order to abide by the statutory criteria and to avoid a constitutional conflict with the Dormant Commerce Clause. Unless the regulations appropriately account for existing technical solutions to address residency authentication, they are merely creating an impossible burden for businesses that cannot be effectively met.
- The regulations also do not address the potential vulnerabilities for global preference mechanisms. For instance, if browser-based signals are sent unencrypted, they are at risk of interception by malicious actors. The mechanisms should be required to address this.

### **3. Requests to Opt-Out of Sale/Sharing [Section 7026]**

We appreciate the modifications made to this Section, including striking the language requiring businesses notify all third parties to whom the business has sold or shared the consumer's personal information, and allowing businesses the option to provide a means by which the consumer can confirm that their request to opt out has been processed.

We maintain the opt-out right should apply prospectively only for ease of implementation, especially in light of the looming enforcement deadline.

In Section 7026(a)(1), the added limitation for processing in frictionless manner should be removed because the alternatives and the benefits to the consumer are unclear.

Proposed Edit:

**Section 7026(a)(1):** 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.~~

### **4. Restrictions on the Collection and Use of Personal Information [Section 7002]**

CJAC recognizes and appreciates the effort that went into modifying this Section. We appreciate that the Board struck the data minimization illustrative examples in this Section as they were overly narrow and would threaten innovation.

The proposed modifications, however, create regulatory ambiguity by continuing to depart from the statute and apply a standard for data collection and use that gives the Agency too much discretion to ignore privacy disclosures and substitute its own judgement about the reasonable expectations of the consumer. While we agree that a consumers' expectations are important to data collection and use practices, the standard must be tied to disclosures made to the consumer.

The proposed modifications also inappropriately mandate extensive analysis even for primary collection purposes in a manner that gives unequal weight to factors other than the business's disclosures to the consumers.

Section 7002(b)(3) of the revised rules overly prescribes what a consumer may or may not expect that the business will use personal information for. 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. This is because the consumer obtains substantial benefit from sharing data across services, such as using data from a reading app to personalize book recommendations in an online store (whether both services are offered by the same business). To the extent this factor is retained, it should focus on whether the use on the different product or service is unexpected and unrelated.

Proposed Edit:

**Section 7002(b)(3):** 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 [an unexpected and unrelated use on a](#) different product or service offered by the business or the business's subsidiary.

In Section 7002(b)(4), 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:

**Section 7002(b)(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.~~

The added factor in Section 7002(b)(5), 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:

**Section 7002(b)(5):** 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 ~~would be unexpected [and offensive]~~ ~~is apparent~~ to the consumer.

### 5. Contract Requirements for Service Providers and Contractors [Sections 7050-7053]

We are thankful to the Board for striking the last sentence of Section 7051(a)(3), which would have required a list of the specific business purpose(s) and service(s) identified in subsection (a)(2), and for modifying the language in Section 7051(a)(8), which would have provided five business days for the service providers/contractors to notify businesses they can no longer meet obligations.

However, we are concerned that Section 7050(e), previously Section 7051(c), continues to propose that all service provider/contractor relationships be converted into third party relationships if the contract is not fully compliant with the rules. This will trigger a host of additional legal obligations which is punitive and unreasonable. A noncompliant contract should be handled as other violations are handled without unwinding legal relationships between private parties, and there should be a reasonable opportunity for businesses to address contract issues.

Moreover, the triggered third-party classification would not reflect the actual relationship between the business and the external party, which might be engaged in an otherwise permitted business purpose that is neither selling nor sharing.

Designating a service provider as a third party also does not accurately reflect the business relationship and likely necessitates a violation of the sale opt out (which would not apply to service provider relationships). The violation of the contract provision, standing alone, is a sufficient penalty. This rule should be eliminated.

Section 7051(c), previously Section 7051(e), and Section 7053(b), would create a potential backdoor requirement that a business must conduct due diligence and audits on its service providers, contractors, and third parties. To the extent the Agency promulgates regulations on when the exemption in CPRA Section 1798.145(i) applies, they should be limited to factors that affirmatively indicate that the external party is violating its obligations – and not impose additional burdens on business to confirm the absence of violations.

Proposed Edits

Sections 7051(e) and 7053(e) should be deleted in their entirety or alternatively revised as follows:

**§ 7051(e):** A business shall take reasonable steps to determine compliance with the terms of the contract with service providers and contractors when the business has reason to believe that a service provider or contractor is using personal information in violation of the CCPA and these regulations. ~~Whether a business conducts due diligence of its service providers and contractors factors into whether the business has reason to believe that a service provider or contractor is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract nor exercises its rights to audit or test the service provider's or contractor's systems might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the service provider or contractor.~~

\*\*\*

**§ 7053(e):** A business shall take reasonable steps to determine compliance with the terms of the contract with third parties when the business has reason to believe that a third party is using personal information in violation of the CCPA and these regulations. ~~Whether a business conducts due diligence of the third party factors into whether the business has reason to believe that the third party is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract might not be able to rely on the defense that it did not have reason to believe that the third party intends to use the personal information in violation of the CCPA and these regulations at the time of the business disclosed the personal information to the third party.~~

## **6. Requests to Delete and Correct [7022-7023]**

We appreciate the flexibility provided to businesses as a result of several changes made to these sections, including Section 7023(c) and 7023(i), among others.

However, the requirement in Section 7022(b)(3), (c)(4) and 7023(c) to send detailed correction and deletion requests to service providers and contractors in all situations is overly burdensome for businesses. There need to be parameters in place for when such a request is impossible to meet or involves disproportionate effort.

Similarly, a business should not be required to provide a consumer with detailed explanations as to why it cannot delete all personal information (particularly when a legal exception applies) (Section 7022(f)(1)), why it cannot provide PI beyond a 12-month period (Section 7024(h)), and when denying correction requests (Section 7023(f)).

Permitting consumers to submit an additional access request to confirm that a business has properly processed a correction request puts an onus on businesses to process repetitive requests in a manner inconsistent with the statute. We again request that Section 7023(j) be deleted. Between the data broker registry and the fact that all California businesses will allow consumers to submit requests, consumers have significant control over their personal information. These additional provisions are unnecessary.

Finally, while we appreciate the changes made to Section 7023(c), which will now allow businesses to delay compliance with the consumer's request to correct, the parameters are not clear. For instance, how



long do businesses have to honor requests? Can businesses deny requests? Do businesses have to store requests until the archive/backup becomes active? Clarification is needed.

#### **7. Requests to Know [Section 7024]**

The modifications did not provide reasonable parameters for requests to know from consumers. While there was a revision to allow businesses to provide only the personal information it has collected in a specific time period when the consumer designates one, this change does not go far enough. If the consumer does not designate a time period, the business must still provide all information collected for unlimited time ranges.

#### **8. Dark Patterns [Section 7004]**

The revised proposed symmetry choice standard 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 language should make 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:

Section 7004(a)(2): Symmetry in choice. 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 would impair or interfere with the consumer's ability to make a choice. Illustrative examples follow.

As for Section 7004(a)(4), the proposed modifications state that businesses cannot "design their [choice architecture] methods in a manner that that would impair the consumer's ability to exercise their choice because consent must be freely given, specific, informed, and unambiguous." This could be interpreted as a backdoor and extra-statutory regulatory requirement to mandate opt-in consent for all data collection and uses. It also creates confusion for businesses already navigating a complex statutory regulatory standard.

The burdens from this confusion are compounded by the continuous delays in finalizing the regulatory standard. The Agency should clear up any potential confusion or regulatory overreach by explicitly stating that the regulations do not intend to mandate an opt-in consent standard beyond what the statute expressly requires and also striking the Section 7004(a)(4) language identified above.

Finally, the dark pattern reference of 7004 (b) is an overly harsh result. Broken links, slow webpages, and vagueness of some of the requirements of Section (a) do not necessarily result or lead to a "dark pattern" conclusion.

#### **9. Notice at Collection of Personal Information [Section 7012]**

We appreciate the modifications made to this Section with respect to the sharing of third party names with consumers.

We again note that for third-party businesses that control the collection of data on another business' premises, Section 7012(g)(3) should permit third-party businesses to provide notice in a reasonable manner that factors in the method of the data collection.

Again, the requirement under Section 7012 to provide unique lists of personal information and third parties for each consumer notice will be extremely burdensome and can be addressed more efficiently for businesses and consumers through the businesses' privacy policies. Section 7012(f) should be struck or modified to reflect this.

#### **10. Notice of Right to Opt-Out of Sale/Sharing of and the "Do Not Sell or Share My Personal Information" Link [Section 7013]**

We urge the Board not to exceed its statutory authority by requiring businesses provide notice to opt-out of sale/sharing in the same way it collects the personal information for that purpose.

Further, the affirmative consent requirement of Section 7013(h) appears nowhere in the statute, conflicts with CPRA's opt-out framework, and should be removed.

#### **11. Limit Sensitive Information and Alternative Opt-Out Links [Sections 7014-7015]**

We maintain the regulations should allow the alternative opt-out link to be in text form without the requirement of an accompanying icon for ease of implementation.

The modified draft regulations also mandate the opt-out icon even though it was 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 for questionable if any consumer benefit.

Proposed Edit:

Section 7015(b):

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.

#### **12. Requests to Limit Use and Disclosure of Sensitive Personal Information [Section 7027]**

Once again, the rules seem to create three distinct categories of consumer harm, with Section 7027(a) referencing a "heightened risk of harm," which is ambiguous in light of the references to "risk of harm" and "greater risk of harm" in Section 7060(c)(3).

As discussed previously, use cases for sensitive personal information should not be preselected for the consumer. The Agency should not require that a single option be presented more prominently than the others. This could interfere with customer choice and information. It also conflicts with the Agency's proposed symmetry standards for consumer choice architecture under Section 7004.24.

Finally, Section 7027(i) should be revised to enable businesses to deny requests for sensitive information from authorized agents if there is reasonable suspicion that it is a fraudulent request.

#### **13. Training [Section 7100]**

The training requirement set forth in Section 7100 appears to expand the scope beyond the law, as it states that businesses must train people handling inquiries on Information practices OR compliance with CPPA on all CPPA requirements. People who handle inquiries on Information Practices, such as inquiries about the NoPP, or Protected Persons, or breach investigations, or HIPAA, may not have any CPPA

handling responsibilities. Businesses should not be forced to train people on CPPA who have no CPPA responsibilities.

#### **14. Audits and Enforcement**

The modified draft rules continue to leave significant problem areas under the audit and enforcement provisions, including:

- As a general matter, neither the modified regulations nor the Board itself addressed probable cause proceedings, agency audits, risk assessments of personal information processing, or the impending expiration of the employment records exemption set forth in CPRA Section 1798.145(m)(1) set for January 1, 2023.
- Section 7302 should be revised to provide the alleged violator an opportunity to cure during the 30-day window between receipt of notice of proceeding and the proceeding.
- Section 7304 should be revised to limit audits to possible violations that are based on reasonable suspicion, and the rules should define “significant risk” under Section 7304(b) or provide examples. The proposed regulations should also be confined to audits of businesses, not individuals. Further, the Agency’s enforcement process and auditing authority need to incorporate more flexibility to be efficient and appropriately balance burdens and costs associated with both.
- The Agency should incorporate a range of enforcement mechanisms into the regulations, consistent with Cal. Civ. Code § 1799.199.45, as other California enforcement bodies have done. Although the CPRA authorizes the Agency to conduct compliance audits, the regulations must place some parameters on this power. An audit is a resource-intensive exercise for both the Agency and the business. Without clearer triggers and limitations, the Agency could conduct broad fishing expeditions, leading to mounting pressure to find some basis for an enforcement action.
- As for Risk Assessments, The CPRA requires businesses to submit these to the Agency on a regular basis under Section 1798.185(a)(15)(B) and instructed the Agency to address this obligation in the rulemaking.

We appreciate the opportunity to further comment on the modified regulations. We stress the importance of providing adequate time to work through feedback on by stakeholders including the business community as well as extending the enforcement deadline. It is in Agency’s and stakeholders’ best interests to have a clear and workable set of regulations which will facilitate compliance and help to avoid unnecessary and unproductive enforcement actions and litigation.

Thank you for your consideration, and we are happy to address any questions you may have about our comments.

Respectfully submitted,



Lusine Chinkejian  
Counsel

---

**From:** Lori Enrico [REDACTED]  
**Sent:** Monday, November 21, 2022 12:08 PM  
**To:** Regulations  
**Cc:** Melanie Salas  
**Subject:** FW: CPPA Public Comment  
**Attachments:** Public Comment Letter.pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Please see the attached public comment for your review. We appreciate the opportunity to contribute to the discussion regarding this proposed regulation.

Sincerely,

Lori L. Enrico  
*Partner*



t: [REDACTED] | f: [REDACTED] | e: [REDACTED]

7522 N. Colonial Ave., Suite 100, Fresno, California 93711

**WARNING/CONFIDENTIALITY:** This electronic message, and any attachment(s) hereto, is covered by the Electronic Communications Privacy Act, 18 U.S.C. sections 2510-2521, and may contain privileged or confidential information; it is intended only for the person(s) identified herein as addressee(s). If the recipient is not an addressee or a person to whom the sender has sent this message, or if the recipient has received this message by mistake, you are hereby notified that dissemination, distribution or copying this message is strictly prohibited and should be immediately deleted with any attachment(s). In such event, please notify the sender immediately by return electronic mail or by telephone at the phone number above. Delivery of this message, and any attachment(s) hereto, to any person other than the intended recipient(s), is not intended to and does not waive any privilege or confidentiality.

JESSICA L. GIANNETTA  
LORI L. ENRICO



PHONE: [REDACTED]  
FAX: [REDACTED]

[REDACTED]  
File No. [REDACTED]

November 21, 2022

***Via Electronic Mail – regulations@cpha.ca.gov***

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

Re: CCPA Public Comment

Dear Mr. Soublet:

On behalf of Giannetta & Enrico, LLP, a law firm that provides comprehensive legal services to financial institutions in the transactional, regulatory, and compliance practice areas, we appreciate the opportunity to submit the following comments on the proposed rulemaking to adopt regulations relating to the California Privacy Rights Act of 2020 (the “Act”).

We enthusiastically support the goal of protecting the privacy of the residents of California, including their data, and we are committed to assisting our banking clients in furthering this goal. We also understand that developing regulations which encompass all types of industries is going to, by necessity, leave little room to address the particular impact those regulations will have on each category of businesses in the state. However, it is imperative to draw your attention to the impact the proposed regulations will have on financial institutions seeking to serve California residents through commercial and business loan products. If the proposed regulations are implemented as currently drafted, it will have *significant unintended consequences* on the ability of financial institutions to serve California businesses, including increased pricing and rates on loans, negative impacts to loan loss reserves, reduced loan approvals, and drastically reduced term lengths for loans.

We ask you to consider the reason for the explicit carve out in §1798.145 for personal information provided to financial institutions which is:

“...collected, processed, sold, or disclosed pursuant subject to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code), or the federal Farm Credit Act of 1971 (as amended in 12 U.S.C. 2001-2279cc and implementing regulations, 12 C.F.R. 600, et seq.)” (collectively, the “Financing Acts”).

This language was, arguably, included to further the overall goal of the Act. However, this carve out is too narrowly tailored because it covers only personal information which is supplied to financial institutions primarily for “personal, family or household” purposes. In contrast, personal information which is supplied to financial institutions primarily for business or commercial purposes (e.g., seeking a small business loan) is not

subject to the Financing Acts, even if these financial institutions are regulated by the foregoing Acts, and undergo numerous government audits and comply with countless federal and state regulations. Consequently, under the current reading of the proposed regulations, financial institutions must offer an opt-out option to consumers who are either seeking to obtain a business loan in their individual name, or (more commonly) consumers who are personally guaranteeing a business loan.

This lack of an exception for allowing a consumer to opt-out from or consent to the selling or sharing of personal information relating to a commercial loan is **dire**. The reasons for this have been repeatedly mentioned in prior public comments. Specifically, financial institutions which obtain personal information from a consumer for the purpose of offering financing (including commercial financing), must evaluate the risk each borrower presents. In doing so, one way to mitigate risk, and create more opportunities for making loans, is for financial institutions to have the ability to unilaterally sell their beneficial interests in the consumer's contractual obligations (i.e., sell the loan to another lender). In other words, the "...secondary marketplace is where ownership of performing and nonperforming receivables (i.e., the asset) are purchased by companies that were not a party to the originating transaction. The secondary marketplace benefits original creditors by allowing them to monetize performing and nonperforming [assets], thereby allowing for business growth and the extension of new lines of credit. Consumers likewise benefit..."<sup>1</sup> Prohibiting this ability of financial institutions to sell commercial loans in the secondary marketplace by allowing consumers to opt-out of, or refuse to consent to, the sale or sharing of their personal information (which is only incidental to the secondary sale) would have a **devastating** impact on the ability of financial institutions to make such loans, particularly small business loans.

We reiterate and strongly support the public comments made previously that state:

"If a consumer's right to opt-out of the sale of their personal information under the CCPA is wrongly interpreted to disallow the transference of the consumer's personal information associated with the sale of their legal obligation, their de-identified legal obligation would be virtually unenforceable. This would disable the secondary marketplace and potentially lead to..." increased foreclosures and decreased extensions of credit for individuals seeking a business loan.<sup>2</sup>

The most recent revisions to the proposed regulations demonstrate progress towards the careful tailoring of the Act. In particular, revised § 7027(m)(6) now provides that a business may use or disclose sensitive personal information without being required to offer consumers a right to limit sharing if it only uses or discloses the sensitive personal information to (among other permitted uses): "perform services on behalf of the business. For example, a business may use information for...maintaining or servicing accounts [or] providing financing..."<sup>3</sup> This exception allows financial institutions to provide the service being requested by the consumer without being unnecessarily impeded by the Act, which benefits everyone. We would request this same principal be applied elsewhere in the regulations.

Therefore, to avoid a catastrophic impact on a financial institution's ability to make business loans, and a resulting devastating blow to California businesses of all sizes, we respectfully request that the Attorney General revise the proposed regulations as set forth more fully below.

///

---

<sup>1</sup> Public Comment W45-21.

<sup>2</sup> Id.

<sup>3</sup> [https://cpa.ca.gov/regulations/pdf/20221102\\_mod\\_text.pdf](https://cpa.ca.gov/regulations/pdf/20221102_mod_text.pdf) (page 52).

## § 7026- New Exception for Already Regulated Financial Institutions

In particular, the Attorney General should further revise §7026 by adding a subsection (l) to the existing proposed regulations. We support and reiterate the prior public commentary relating to financial institutions which calls for a safe harbor for: “already comprehensively regulated businesses like financial institutions. We note that, unlike unregulated businesses, financial institutions undergo regulatory compliance examination by state and federal agencies” already, and we seek “...clearer verbiage to carve out an exception for the financial industry.”<sup>4</sup>

As discussed above, there are already carve-outs in §7027 for businesses to perform maintenance or servicing of accounts or to provide financing without providing a right to limit sharing, and there is already a similar exception to the right to delete in § 1798.105(d)(1), which provides that a business need not comply with a consumer’s request to delete personal information if it is reasonably necessary for the business to:

“...complete the transaction for which the personal information was collected... provide a good or service requested by the consumer, or reasonably anticipated by the consumer within the context of a business’ ongoing business relationship with the consumer, or otherwise enforce or perform a contract between the business and the consumer.”

Accordingly, by adding nearly identical language from §7027 and §1798.105 to §7026, the Attorney General can make it clear an already regulated financial institution need not provide consumers with the choice to opt-out of sharing personal information when selling or sharing that information is necessary for certain financing purposes. As a result, the revised Act would simply allow the application of exceptions already permitted in other areas of the privacy regulation to apply to this section, too. This would enable financial institutions to perform the services which were contracted by the consumer, without any negative impact on the privacy of the consumer. This new subsection could state something similar to the following:

*“(l) Financial institutions which are already regulated by the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code), or the federal Farm Credit Act of 1971 (as amended in 12 U.S.C. 2001-2279cc and implementing regulations, 12 C.F.R. 600, et seq.), shall not be required to provide consumers with the choice to opt-out, or to comply with requests to opt-out, of the sale or sharing of the consumers’ personal information, if such sale or sharing is reasonably necessary to: (i) maintain or service accounts, or provide financing to consumers; or (ii) complete the transaction for which the personal information was collected, provide a service requested by the consumer, or reasonably anticipated by the consumer within the context of a business’ ongoing business relationship with the consumer, or otherwise enforce or perform a contract between the business and the consumer. This subsection shall apply to personal information supplied by a consumer to financial institutions whether such personal information is actually subject to the foregoing regulations or not.”*

///

///

---

<sup>4</sup> Public Comment W117-2; Public Comment W131-1.

### § 7026- New Exception for All Businesses for Certain Uses

Alternatively, if the Attorney General is not able to make an explicit exception for financial institutions as requested above, please consider revising §7026 to allow for certain permitted uses of personal information without the need to provide consumers with the choice to opt-out. This could be achieved by adding a subsection (l) to the existing proposed regulations of §7026 stating something similar to the following:

*“(l) Businesses shall not be required to provide consumers with the choice to opt-out, or to comply with requests to opt-out, of the sale or sharing of the consumers’ personal information, if such sale or sharing is reasonably necessary to: (i) maintain or service accounts, or provide financing to consumers; or (ii) complete the transaction for which the personal information was collected, provide a service requested by the consumer, or reasonably anticipated by the consumer within the context of a business’ ongoing business relationship with the consumer, or otherwise enforce or perform a contract between the business and the consumer.”*

### § 7001. Revised Definition for “Sell,” “Selling,” “Sale,” or “Sold”

In addition to revising §7027, or as an alternative, the Attorney General should revise the definitions of "sell," "selling," "sale," or "sold" already contained in § 1798.40 by amending § 7001.<sup>5</sup> The reasons for the need to revise the definitions are primarily two-fold.

First, the definitions should be revised to bring them in line with already existing regulations which govern financial institutions’ responsibilities when disclosing personal information. We reiterate and support the prior public comment on this issue, which called for the exclusion from the current definition of "sell," "selling," "sale," or "sold" those “...items that are subject to the general exceptions in 15 U.S.C. §6802(e) [also known as the Gramm-Leach-Bliley Act]...” but we would respectfully request that those items apply to the personal information being supplied by the defined term “consumer” under the proposed regulations, and not limited to the defined term “consumer” under the Gramm-Leach-Bliley Act.<sup>6</sup> This is due to the fact that the term “consumer” under the Gramm-Leach-Bliley Act only applies to those who are seeking financing primarily for personal, family, or household purposes, and does not include those who are seeking a business loan. Again, we reiterate and support the prior public comment which stated that these exclusions “...are vital to the functioning of the secondary market activity that provides capital for financial products and services and are subject to extensive federal oversight,” and that this is true regardless of the purpose for which the loan was obtained.<sup>7</sup>

As already stated in the Gramm-Leach-Bliley Act, the proposed regulations here should specifically allow the following scenarios relating to the selling or sharing of personal information supplied to a financial institution regardless of whether that information was provided for a personal, family, or household loan, or a business loan:

“(1) as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with-

(A) servicing or processing a financial product or service requested or authorized by the consumer; (B) maintaining or servicing the consumer's account with the financial

<sup>5</sup> § 7001 already states that the definitions contained in § 7001 are “in addition to the definitions set forth in Civil Code section 1798.140” so only amending § 7001 would be necessary and appropriate.

<sup>6</sup> Public Comment W186.16.

<sup>7</sup> Id.



institution, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or (C) a proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer”<sup>8</sup>

Second, in addition to the need to include business loans within the protected carve out set forth above, it is also imperative to revise these definitions to clarify that the terms only apply when “the primary object of the ‘sale,’ (i.e., the thing of value for which ‘monetary or other valuable consideration’ is received) is the personal information itself.”<sup>9</sup> We adamantly concur with prior public comments identified as W45-21, which stated:

“This clarification would address the common situation in which a consumer's contractual obligation is sold, typically as part of a portfolio, and it is the value of the obligation, rather than the consumer's incidental personal information, that is the object of the sale. This concern was raised at the Sacramento and Riverside Public Hearings: Many financial institutions regularly sell portfolios within their business. So, for example, a credit card portfolio or a loan portfolio, another example would be like a delinquent account portfolio. In those cases, the personal information associated with those accounts is transferred with the commercial sale of that portfolio. The terms of that customers' contract don't change. It would really be helpful if the regulations would clarify that selling those types of portfolios -- portfolios of that nature and transferring the corresponding personal information to some commercial purchasers [are] excluded from the definition of sale. These types of commercial sales are common in the financial industry, and they don't impact the customers directly.<sup>10</sup> The CCPA defines sale to include any data transfer for monetary or other valuable consideration. It's not clear whether the monetary consideration must be received for the purchase of personal data as opposed to some other business arrangement where the data is not the subject of the exchange<sup>11</sup>...For these reasons, [we] respectfully request clarification that a "sale" of personal information does not occur when it is the obligation with which it is associated that is the asset for which "monetary or other valuable consideration" is received.

Similarly, [we] respectfully request the Attorney General clarify that the sale of a consumer's contractual obligation is not considered to be the sale of that consumer's incidental personal information for purposes of the CCPA. This clarification will confirm our understanding that the additional compilation, disclosure, documentation, and compliance requirements... do not apply to financial institutions that do not buy, receive, sell, or share personal information except as incidental to the contractual obligation that is the object of the sale or transfer.”

Thus, incorporating all of the above, the revised definition in §7001 could be similar to the following new subsection:

---

<sup>8</sup> 15 U.S.C. §6802(e).

<sup>9</sup> Public Comment W45-21.

<sup>10</sup> Transcript, Public Hearing on the California Consumer Privacy Act (CCPA), Riverside, CA, January 24, 2019, p. 9. <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-forum-riverside-012419.pdf>? (last accessed November 20, 2019).

<sup>11</sup> Id at page 30.

*“(nn) “Sell,” “selling,” “sale,” or “sold” does not include the selling, renting, releasing, disclosing, disseminating, making available, transferring, sharing, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information: (1) as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with: (A) servicing or processing a financial product or service requested or authorized by the consumer; or (B) maintaining or servicing the consumer’s account with the financial institution, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or (C) a proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction requested or authorized by a consumer; or (D) any other general exception set forth in 15 U.S.C. §6802(e) which shall be interpreted to apply to a consumer as that term is defined in these regulations, and not limited to the definition of consumer set forth under 15 U.S.C. §6809(9); or (2) when the contractual obligation with which the personal information is associated is the asset for which monetary or other valuable consideration is received, and the sale of personal information is only incidental thereto.”*

#### **§ 7001. Revised Definition for “Personal information”**

In addition to revising §7027, and revising the definitions of “sell,” “selling,” “sale,” or “sold” under §7001, or in combination therewith, the Attorney General should revise the definition of “personal information” under §7001 as well.

As previously mentioned in Public Comment W24-2, “[c]ertain information must be obtained and shared (and retained under state or federal law or regulation) when a financial transaction takes place. Without such collection, retention and sharing there could be no ATM, Debit Card, Credit Card or check writing or check cashing for example.” Consequently, there needs to be clarification that certain information that is necessary for a financial transaction should not fall under the definition of the term “personal information” as set forth in the proposed regulations.

Thus, in making this clarification, a revised definition of “personal information” in §7001 could be similar to the following new subsection:

*“(oo) “Personal information” does not include consumer information which is necessary to process, effect, enforce, facilitate or administer a financial transaction.”*

#### **§ 7305. New Section Delaying Enforcement Under Article 9**

Understanding that final regulations will not be adopted by the statutorily mandated deadline we request that the regulations not be enforceable until one year from the date of final adoption of this rulemaking. Businesses subject to the Act would have been given one year to implement the requirements of the regulations before enforcement of the regulations began. Accordingly, we request that the regulations become enforceable one year after the date the regulations are finalized. This can be done by adding a new section, §7305, to Article 9 of the proposed regulations.

///

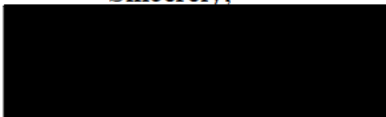
///

## Conclusion

Giannetta & Enrico, LLP, recognizes the importance of consumer privacy in today's increasingly technology-based business world. While some industries lack sufficient regulation, financial institutions are already subject to comprehensive federal regulation, including robust and effective privacy laws. In addition, in order for the Attorney General to avoid imposing catastrophic unintended consequences on the same Californians it is seeking to protect, carve-outs in the proposed regulations for financing activities and secondary market sales are crucial. We respectfully ask that the proposed regulations be further revised as requested herein in order to protect not only the privacy of consumers in California, but also their opportunities to obtain financing for their businesses as well.

We thank you for the opportunity to provide comments on the proposed regulations and are available to discuss any questions you may have regarding the foregoing.

Sincerely,

A solid black rectangular redaction box covering the signature of Lori L. Enrico.

Lori L. Enrico

---

**From:** Melissa O'Toole [REDACTED]  
**Sent:** Monday, November 21, 2022 1:08 PM  
**To:** Regulations  
**Cc:** [REDACTED]  
**Subject:** CPPA Public Comment  
**Attachments:** PIFC Updated CPPA Regulation Comments 11212022.pdf

**Importance:** High

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good afternoon,

Attached, please find the updated comments from the Personal Insurance Federation of California (PIFC) to the CPPA's Notice of Modifications to text of proposed California Privacy Rights Act (CPRA) regulations.

Thank you,

**Melissa O'Toole**  
Legislative and Communications Manager  
Personal Insurance Federation of CA

**C:** [REDACTED]  
**W:** [www.pifc.org](http://www.pifc.org)  
**E:** [REDACTED]  
1201 K Street, Suite 950  
Sacramento, CA 95814





**Date:** November 21, 2022

**To:** Members, California Privacy Protection Agency

**SUBJECT:** COMMENTS ON THE AMENDED PROPOSED REGULATIONS UNDER THE CALIFORNIA PRIVACY RIGHTS ACT OF 2020

Dear Members of the Board,

The Personal Insurance Federation of California (PIFC) is a statewide trade association that represents seven of the nation's largest property and casualty insurance companies (State Farm, Farmers, Liberty Mutual Insurance, Progressive, Mercury, Nationwide and Allstate as well as associate members CHUBB, CONNECT by American Family Insurance, NAMIC and Kemper) who collectively write the majority of personal lines auto and home insurance in California.

We greatly appreciate the opportunity to provide comments regarding the amended proposed regulations that the California Privacy Protection Agency ("Agency") released on June 8<sup>th</sup>, 2022.

We continue to emphasize the importance of understanding that insurance is a highly regulated industry nationally, but particularly in California. Insurers are subject to federal privacy laws under the Graham Leach Bliley Act (GLBA), and the Insurance Information and Privacy Protection Act in California specifically. Conformity with both of these privacy structures has been enforced and overseen by the California Department of Insurance up to and through this point in time.

The state's Insurance Commissioner heads the largest consumer protection agency in the United States with over 1300 staff and a \$300 million budget. Current law provides the commissioner with unrestricted access to the records, employees, officers, and contractors of any insurer. The commissioner is required to investigate the compliance of an insurer (commonly referred to as a "market conduct examination") periodically (generally every five years) but is permitted to examine an insurer at any time. Notably, insurers must reimburse the commissioner for the costs incurred conducting an examination. Few industries have the routine presence of a regulator with the power of the Insurance Commissioner.

There is serious timeliness concern, particularly when paired with the failure of the legislature to address the business-to-business and employee exemptions of CCPA sunseting at the end of this year. The subject matter of these regulations is complex and serious and should not be rushed, a sentiment voiced repeatedly by members of the Board during the October 28<sup>th</sup> meeting. While the changes made to the proposed regulations make some improvements, they continue to require work. We stand with the rest of the California Chamber of Commerce in requesting that the Agency delay the adoption of regulations for an additional 6 months and postpone the enforcement to 12 months from the adoption of the final regulations. The current timeline simply does not give reasonable or adequate implementation time for businesses.

Regarding the components of the updated regulations, PIFC respectfully submits the following general comments to help inform the future regulations. These are intended to be insurance industry specific comments that should be considered in addition to the comments the Agency will receive from the broader business community, which also reflect input from insurers.

### **Existing State and Federal Law Exemptions**

Due to the extensive oversight that insurers are already subject to, a decision was made during the adoption of the California Consumer Privacy Act (CCPA) that those already subject to federal privacy law would not be subject to certain provisions of the CCPA (SB 1121 (Dodd) Chapter 735, Statutes of 2018). The importance of these exceptions was critical to ensure conformity and compliance across multiple industries. It is for those same reasons that similar exemptions exist in the American Data Privacy Protection Act (H.R. 8152), currently being considered before the House of Representatives.

Notably, the draft regulations do not have the exemption explicitly enumerated. Exemptions structured similarly to those under California Civil Code Section 1798.145 are essential to companies maintaining their compliance with other laws and reflect longstanding and complex consumer protections. We have noted that the proposed regulations make multiple references to companies having the abilities to assert defenses to claims under the regulations if they have a protection through the exemptions under the statutes, despite not explicitly reiterating the exemptions. We take those clauses (7022(f)(1); 7023(f)(1); 7024(e)) to reflect the Agency's intent to adhere to and honor the protections enumerated under the existing structures.

### **Delay in Enforcement**

As stated above, the timing remains a critical concern for our industry. The California Privacy Rights Act required rulemaking to be finalized by July 1, 2022 and enforcement of the rules to begin a year later *Cal. Civ. Code § 1798.185(d)*. It is understandable that there are significant demands upon the CPPA and the delay in initiating the current rulemaking. The CPPA needs to clarify its plans for enforcement and effective dates of the CPRA regulations. Only some of the anticipated regulations have been drafted, with some of the most complex and potentially complex proposed rules yet to be promulgated (*i.e.*, *Insurance Clarification section*). The Agency should clarify that enforcement, in line with the spirit of the CPRA text, make recommendations at least by July 2024, and the rules should take effect no sooner than January 2024. This will provide businesses enough time to implement the complex requirements.

On November 8, 2021, the California Department of Insurance ("Department") sent a letter to the Agency asking that "the Agency provide the Department with the opportunity to work with the Agency before the adoption of any regulation that would implement the insurance privacy subdivision of the Civil Code [Section 1798.185(a)(21)]." The Department explained that it:

*Participates in the National Association of Insurance Commissioners ("NAIC"), which serves as a regulatory college and policy coordination body for the insurance commissioners of the states and territories of the United States. Among the NAIC functions is the development of Model Acts which membership may adopt. California's IIPPA is based on the NAIC Insurance Information and Privacy Protection Model Act; NAIC Model Act #670.*

*The NAIC is in the process of soliciting regulator and stakeholder comments on revisions to Model #670. For the last two years, CDI has participated in a working group of insurance regulators charged with determining the applicable scope of privacy protections for insurance consumers. The working group report is scheduled to be presented this December and will likely recommend amendments to Model #670. Because California's IIPPA is based on Model #670, the IIPPA will likely be amended in the next 2-4 years, after the adoption of revisions to the NAIC Model, or development of a new model. The PNPI regulations are based on the IIPPA, and are also likely to be revised. Due to the impending amendment of applicable insurance privacy statutes, the Department respectfully requests that the Agency provide the Department with the opportunity to work with the Agency before the adoption of any regulation that would implement the insurance privacy subdivision of the Civil Code. Because the NAIC is actively working to amend Model #670, which will affect the IIPPA and related PNPI regulations overseen by [the Department], close coordination between the Department and the Agency is critical. This will avoid duplicative efforts on the part of the Agency and the Department, and promote certainty on the part of consumers and regulated entities.*

The Agency and California Attorney General should declare a moratorium on enforcement of CCPA/CPRA regulations in the insurance sector until after the review and rulemaking done in connection with the above and required by 1798.185(a)(21) are completed. Because the regulations will be integral to determining how insurers must comply with the statute, the moratorium should include enforcement of the CCPA/CPRA statutory provisions.

Ideally, the moratorium should cover:

- Any enforcement activity until the insurance-specific regulations are effective; and
- Any retroactive enforcement relative to acts and omissions prior to the effective date of the regulations.

There is concern that insurers will invest significant time and resources on compliance decisions that will almost certainly need to be revisited when the insurance-specific regulations are issued. This will be confusing for Californians, who already enjoy significant privacy protections under Cal. Ins. Code § 791, *et seq.*, the related privacy regulations (10 CA ADC § 2689.1, *et seq.*), and the California Financial Information Privacy Act, Ca. Fin. Code § 4050 *et seq.* Together, these laws have, for decades, provided Californians with notice, choice, disclosure, and correction rights, not unlike those found in the CCPA/CPRA.

### **Notice at Collection**

Some of the initial concerns we raised in this section were addressed in the initial amendments, however there are continued concerns. The Amendment Regulations mandate the notice given at the time of collection to detail “the length of time the business intends to retain each category of personal information...or if that is not possible, the criteria used to determine the period of time it will be retained.” *Amended Regulation § 7012(e)(4)*. Such prescriptive requirements are difficult to comply with

because businesses deal with various factors such as the consumer relationship, transaction duration, and other legal requirements. A specified data element could have various retention periods under the law.

### **Business Practices for Handling Consumer Requests**

There are several issues under these sections that raise concerns for implementation to insurers.

The first being that insurers already have mechanisms and procedures in place to ensure that the information on their consumers is as up to date as possible. The procedural burdens that the regulations outline would delay and complicate the existing practice, which would harm consumers. Insurance is an industry that relies on accuracy of information at its core. Industries which already have existing structures to allow consumers to update their names, addresses, marital status, and other personal information should not be compelled to adopt a system which creates unnecessary and damaging distance and delay.

To the point above, “inaccurate information” is vague as to what information the consumer has the right to correct. Within the insurance context, while personal information such as name, date of birth, and marital status are easily updated. However, there is critical information, such as an individual’s driving record, which cannot and should not be corrected without a showing of inaccuracy by the consumer. The burden should not be placed exclusively on the insurer due to insufficient documentation. Information regarding driving records is collected and reported by the DMV, and a request to correct such information should place the burden on the consumer to show that the information is, in fact, incorrect.

Finally, throughout Article 3 of the amended proposed regulations there are references to business exemptions under “subsection 1” including in sections of the Article which contain no subsection 1. For clarity those sections must include clearly defined reference sections, and the exemptions included should conform with the existing exemptions under the CCPA at Civil Code Section 1798.145.

### **Service Providers, Contractors, and Third Parties**

The requirements under Sections 7051(a) and 7053(a) for specific descriptions of services or purposes of data processing provides no greater protection to Californians than referencing contracts generically. In fact, given the potentially thousands of contracts that must be amended by a business, adding this specificity requirement will only serve to extend the time by which the business will be able to implement the required contractual amendments. The specificity requirement will frustrate an efficient means of compliance and provide absolutely no added protection to California consumers.

A business should not be responsible for the compliance of another entity that is not fully under their control. If there is an existing contract between two companies, one should be able to rely on a third party’s compliance with the terms of a contract unless given reason to believe that the third party is not in compliance. Section 7051(e) of the regulations places an unreasonable burden on the company to monitor third parties. This is especially true since third parties are obligated by Section 7051(d) to comply not only with the regulations, but also the terms of the contract required by the CCPA. Section 7051(e) will only serve to



mandate regular and unnecessary audit of third parties, diverting resources from more meaningful efforts to protect the privacy and security of personal information.

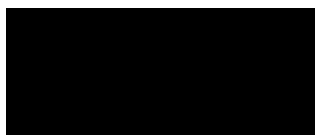
### **Definitions**

Finally, there are certain terms used throughout that either require more explanation in the way that they would be used in their application, or clarity in their definition. For example, dark pattern is a term that was discussed extensively on the October 28<sup>th</sup> meeting, is a term that continues to be a matter of academic discussion, and would require explicit clarity if companies were to be held to a compliance standard. Currently, that is not present. A term that simply requires additional clarity and definition would be “unstructured data”. We appreciate your attention on these points.

For insurers, the challenge of multiple regulators promulgating regulations, examining conduct, and taking enforcement actions is significant. PIFC is hopeful that the Agency will recognize the existing state and federal rules that insurers already comply with, and that avoiding unnecessary, duplicative, and conflicting regulations will be a core principle. Given the complexity and cost of compliance with CPPA and CPRA, our members also seek flexibility wherever possible and appropriate.

We look forward to working collaboratively with the Agency and Board to develop fair regulations that can be implemented in a manner that best serves Californians.

Sincerely,



Allison Adey  
Legislative Advocate  
Personal Insurance Federation of California



Christian J. Rataj  
Senior Regional Vice President  
National Association of Mutual Insurance  
Companies

---

**From:** MacGregor, Melissa [REDACTED]  
**Sent:** Monday, November 21, 2022 1:15 PM  
**To:** Regulations  
**Cc:** Chamberlain, Kim  
**Subject:** CCPA Public Comment  
**Attachments:** California Privacy Regulation Letter - Nov 21, 2022.pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

SIFMA is pleased to provide the following comments on the CCPA modified proposed privacy rulemaking under the CPRA. Please let me know if you have any questions.

Melissa MacGregor  
Managing Director & Associate General Counsel  
SIFMA  
1099 New York Ave., Suite 600  
Washington, DC 20001  
M: [REDACTED]  
O: [REDACTED]



November 21, 2022

Submitted via email: [regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

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

**Re: CCPA Public Comment for CPRA Regulations**

Dear Mr. Soublet,

The Securities Industry and Financial Markets Association (“SIFMA”)<sup>1</sup> appreciates the opportunity to respond to the California Privacy Protection Agency (“CPPA”) Modified Text of Proposed Regulations dated November 3, 2022 (the “Modified Proposed Regulations”) that modifies the previously proposed regulations published on July 8, 2022 as required under the Consumer Privacy Rights Act of 2020 (“CPRA”).<sup>2</sup> SIFMA previously commented on the initial proposed regulations dated August 18, 2022 (“Initial Letter”)<sup>3</sup> and the comments below reflect some of those same comments as well as comments on the Modified Proposed Regulations. SIFMA appreciates the continued work the CPPA has done to bring public attention to consumer privacy issues and work with companies to achieve a higher level of consumer protection.

SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets, including a significant presence in California. SIFMA has 24 broker-dealer and asset manager members headquartered in California. Further, there are approximately 384 broker-dealer main offices, nearly 40,000 financial advisers, and 93,522 securities industry jobs in California.<sup>4</sup>

---

<sup>1</sup> The Securities Industry and Financial Markets Association (SIFMA) is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's one million employees, we advocate on legislation, regulation and business policy affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit <http://www.sifma.org>.

<sup>2</sup> [https://coppa.ca.gov/regulations/pdf/20220708\\_npr.pdf](https://coppa.ca.gov/regulations/pdf/20220708_npr.pdf)

<sup>3</sup> SIFMA Letter to California Privacy Protection Agency (August 18, 2022) (available at <https://www.sifma.org/wp-content/uploads/2022/08/California-Privacy-Regulation-Letter.pdf>).

<sup>4</sup> <https://states.sifma.org/#state/ca>

SIFMA urges the CPPA to carefully consider the costs associated with potentially overly prescriptive regulations both for businesses and ultimately for customers. As we did previously, the below comments highlight several of the proposed requirements which may do little to protect investors, but would be costly to comply with. We are only about one month away from the January 1, 2023, the compliance date for the CPRA, thus making any new obligations inordinately costly at this late date. As such, SIFMA urges the Commission to consider eliminating any requirements that exceed the CPRA mandate from the Modified Proposed Regulations.

SIFMA continues to remain concerned about the expiration of the employee and business-to-business (“B2B”) data exemptions in the CPRA. If, or when, the exemptions expire, the CPRA and its regulations will apply to employee personal information and personal information belonging to an employee or an individual associated with another legal entity involved in a commercial transaction with a business (e.g., B2B contact details). The most recently proposed regulations do not address requirements for responding to requests from employees and B2B contacts. Without specific guidance, applying the CPRA and its regulations to employee and B2B data will create unintended consequences and compliance problems which will be compounded by the new obligations that would be imposed by the Proposed Regulations.

**1. The required business purpose disclosures in agreements and related requirements are impracticable. (Sections 7051(a)(2), 7051(a)(7) and 7053)**

SIFMA continues to be concerned about the provisions that unnecessarily expand on the requirements of the CRPA including Section 7051(a)(2) of the Modified Proposed Regulations which requires businesses to identify in each service provider or contractor agreement the specific business purpose for which personal information is disclosed. The draft regulations would require an impracticable amount of contract remediation to update executed contracts with this information. Further, Section 7053 of the Modified Proposed Regulations requires the same information for third party agreements, which also goes beyond the statute’s requirements and is an impracticable task.

Also Section 7051(a)(7) states that “Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider’s system and regular internal or third-party assessments, audits or other technical operational testing at least once every 12 months.” The ability to do this has significant impacts on license agreements and contractual provisions, intellectual property and security with service providers, much less the ability to create such testing program. SIFMA urges the CPPA to consider require an annual certification of compliance in lieu of an audit.

**2. The Modified Proposed Regulations disregard the statutory language allowing businesses to use Sensitive Personal Information (SPI) for specific purposes. (Section 7027)**

In some sections, the Modified Proposed Regulations contravene and narrow the scope of the statutory language, effectively disregarding CPRA Section 1798.121(a)-(b), which permits a business to use a consumer’s SPI for uses that are “necessary to perform the services or provide

the goods reasonably expected by an average consumer who requests such goods or services,” even after receipt of a consumer’s request to limit. The impact of this overreach will have significant adverse effects on businesses and impair a company’s ability to establish a strong compliance program. The CPPA should amend this language to coincide with the CPRA.

The following examples demonstrate these challenges:

- In Section 7014(h), the draft regulations purport to impose a springing consent requirement with respect to any use, outside the eight limited uses defined by Section 7027, of SPI collected at a time when a business did not have a notice of right to limit posted.
- As a notice of right to limit is not required until January 1, 2023 (and only if the business is collecting SPI for the purposes of inferring characteristics), any personal information collected prior to January 1, 2023, absent consumer consent, may not be used for any purpose other than one of the eight purposes defined by Section 7027.
- Similarly, in Section 7027(g)(1), the draft regulations require that, upon receipt of a request to limit, a business must cease to use and disclose SPI for any purpose other than the eight purposes listed in Section 7027.
- This is a restriction that conflicts with the language in 7027(a) and in 1798.121(a)-(b) that allows uses that are “necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services.”

**3. The requirement to take consumers to a specific section of a privacy policy is unworkable and should be deleted. (Section 7012(f))**

Section 7012(f) of the Modified Proposed Regulations requires a business that collects personal information online to provide the notice at collection by providing a “link that takes the consumer directly to the specific section of the business’s privacy policy that contains the information required in subsection (e)(1) through (6).” The section continues by stating that directing the consumer to the beginning of the privacy policy or to any other section without the required information will not satisfy the notice at collection requirement.

This requirement is overly prescriptive, burdensome, and impracticable. The notice at collection must contain a link to the privacy policy. Additionally, the notice at collection is more tailored to the products or services requested by the consumer, thus seems to require every notice of collection to contain different links to varied sections of the privacy policy which would be confusing for consumers and extremely challenging for businesses. This requirement should be deleted.

**4. Downstream notification of opt-out requests to all third parties is operationally challenging or impossible. (Section 7026(f)(2))**

Section 7026(f)(2) requires a business to notify all third parties to whom the business has sold or shared a consumer's personal information of a consumer's request to opt-out of sale/sharing and to forward the consumer's opt-out request to "any other person with whom the person has disclosed or shared the personal information." Both requirements go beyond the requirements of the statute and would be technically challenging at the device level (whether in connection with a one-off device interaction or in response to a global privacy control).

Further, the requirement to forward a consumer's request to any person with whom the person has disclosed or shared the information does not take into consideration lawful disclosures to service providers, contractors, law enforcement, government agencies, or disclosures to other businesses or individuals pursuant to an explicit request or direction from the consumers to make the disclosure. These requirements go beyond the statute and are operationally difficult or impossible due to technological and practical limitations.

In addition, the CPPA has still not addressed situations where a prospective customer becomes a customer. Businesses need clarity on how to transition customer preferences in these cases. Consent should not be required where an individual becomes a customer under the Gramm-Leach-Bliley Act ("GLBA") and the exception applies.

**5. The requirement to delete personal information from archived or back-up system is expressly excluded from the CPRA. (Sections 7022(b) and (d))**

Section 7022(b)(1) of the Modified Proposed Regulations requires businesses to delete a consumer's personal information from its existing systems except "archived or back-up systems," seemingly indicating that requests to delete do not trigger a requirement to delete personal information on archived or back-up systems. To the contrary, Section 7022(d) states that a business that stores any personal information on archived or back-up systems "may delay compliance with the consumer's request" until the archived or back-up system is "restored to an active system or is next accessed or used for a sale, disclosure, or commercial purpose."

SIFMA requests that the CPPA clarify whether (1) a business is never required to delete personal information stored on archived or back-up systems (as long as it remains on such archived or back-up systems), OR (2) a business has a requirement to delete personal information on archived or stored systems; however, that requirement isn't triggered unless, or until, a business activates that system or accesses, sells, discloses, or uses such data for a commercial purpose.

Additionally, the CPPA should clarify that "access" does not include *de minimis*, temporary, or transient access for maintenance, information security, fraud, system improvement, and other purposes that do not require length or permanent access nor use or disclosure of personal information outside of the limited purposes mentioned.

The Proposed Regulations should be amended to mirror the requirements in Section 1798.100(d) of the CPRA.

**6. The provisions that unnecessarily shift liability away from service providers. (Section 7051(c) and Section 7053(b))**

Section 7051(c) and Section 7053(b) of the Modified Proposed Regulations state that “[w]hether a business conducts due diligence of its” service providers, contractors, or third parties “factors into whether the business has reason to believe” the service provider, contractor, or third party is using personal information in violation of the CCPA/CPRA. Further, both provisions cite an example where a business that never enforces the terms of its contract nor exercises its rights to audit or test might not be able to rely on the defense that it did not have reason to believe that the service provider, contractor, or third party intended to use the personal information in violation of the CCPA.

These provisions go beyond the CPRA and shift nearly all service provider, contractor, and third-party liability to the business. Moreover, the provisions do not discuss what level of due diligence is required to prevent the shifting liability. As a result, these provisions should be struck or amended and clarified such that businesses know what level of due diligence is required to prevent the shifting liability.

**7. CPPA should expressly allow self-service portals for all types of requests. (Section 7024(g))**

Section 7024(g) allows businesses with password-protected accounts to use a self-service that allows consumers to access, view, and receive a portable copy of their personal information. This section should be expanded to also expressly allow consumers to request to delete or request information.

**8. The consumer opt-in provisions are unnecessarily onerous on businesses. (Section 7028).**

Section 7028(a) would require a two-step process for sharing/sale and requests to opt-in for use and disclosure of sensitive personal information. This could potentially be an onerous requirement depending on what is required as a second confirmation step. The CPPA should confirm that the requirement is satisfied if, for example, the consumer clicks a button or check box and then clicks submit.

**9. The Effective Date for the Rule Should be No Earlier Than January 2024**

SIFMA encourages the CPPA to delay the effective date and enforcement of any final CPRA rules until January 2024. Such requirements should only apply to data collected on or after the compliance date to ensure that firms have adequate systems and controls in place to comply with the new requirements. To date, only a portion of the CPRA regulations have been proposed and some critical and potentially complex regulations including automated decisionmaking are still forthcoming. The operational challenges highlighted in this letter clearly indicate that additional time will be needed for companies to fully and responsibly implement new requirements given the complexity of these requirements. Requiring businesses to attempt to

comply prior to that time will lead to confusion and sloppy execution that will only harm businesses and consumers alike.

\* \* \* \* \*

SIFMA and its members appreciate the opportunity to provide these comments and welcome further discussion. Please reach out to Melissa MacGregor at [REDACTED] with any questions or to schedule a meeting.

Sincerely,

[REDACTED]

Melissa MacGregor  
Managing Director & Associate General Counsel

cc: Kim Chamberlain, Managing Director, State Government Affairs, SIFMA



---

**From:** Snell, James (Jim) (PAO) [REDACTED]  
**Sent:** Monday, November 21, 2022 2:41 PM  
**To:** Regulations  
**Subject:** CCPA Public Comment  
**Attachments:** 2022 11 21 Client CPRA Further Regulation Comments.pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Please find attached a client's comments to the Modified Draft of Proposed CPRA Regulations. We appreciate the opportunity the Agency has provided for comments. Best,

**James (Jim) Snell | Perkins Coie LLP**

**PARTNER**  
3150 Porter Drive  
Palo Alto, CA 94304-1212  
M. +1 [REDACTED]  
D. +1 [REDACTED]  
F. +1 [REDACTED]  
E. [REDACTED]



***Perkins Coie is ranked Band 1 in Privacy & Data Security: Litigation by Chambers USA.  
Ranked among the best in the nation for Privacy & Data Security Law by Chambers USA.***

---

NOTICE: This communication may contain privileged or other confidential information. If you have received it in error, please advise the sender by reply email and immediately delete the message and any attachments without copying or disclosing the contents. Thank you.



3150 Porter Drive  
Palo Alto, CA 94304-1212

T +1  
F +1



PerkinsLoie.com

November 21, 2022

James G. Snell



D. +1  
F. +1



**VIA EMAIL**

California Privacy Protection Agency  
Attn: Brian Soublet  
2101 Arena Blvd.  
Sacramento, CA 95834  
[regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

**Re: Comments on Agency's Modified Draft of Proposed CPRA Regulations**

Dear Mr. Soublet:

Please find below comments on behalf of an anonymous client to the California Privacy Protection Agency's ("Agency's") proposed modifications to the draft California Consumer Privacy Act ("CCPA") regulations (hereinafter, "modified proposed regulations"). To be clear, these comments are not provided on behalf of Perkins Coie LLP, and do not necessarily reflect the views of Perkins Coie LLP, but instead reflect comments from a client who asked that we submit such comments on their behalf. We thank the Agency for the opportunity to provide these further comments.

**1. Restrictions on the Collection and Use of Personal Information (Sec. 7002)**

We commend the Agency's efforts to revise and improve this section of the regulations such that they appropriately recognize the role of consumer disclosures in determining the scope of permitted processing. This modification not only helps to align the regulations with longstanding privacy principles and laws in other jurisdictions, but also rightfully couches the permissible processing analysis in terms of "reasonable" consumer expectations as opposed to "average" ones.

However, one revision to this section causes concern regarding the distinction between processing by the business itself and that done by a service provider or contractor. Specifically, the statement in Section 7002(b)(5)—that a factor in determining whether processing is "consistent with the reasonable expectations of the consumer(s)" is the degree to which a service provider's or contractor's involvement therein is apparent to the consumer—suggests, we think incorrectly, that a service provider's or contractor's processing is somehow less "expected" and, in turn, less likely to be lawful, than the same processing when done by the business itself. Such a distinction with respect to service providers and contractors, in particular, is incompatible with the very nature of such entities under the law. By definition, service providers and contractors operate according to

Brian Soublet  
 November 21, 2022  
 Page 2

the written instructions of the business, acting on its behalf, and at its direction, pursuant to a contract. And service providers and contractors are often in a better position to provide privacy protections to personal information. Accordingly, the degree of a service provider's or contractor's involvement in the collection or processing of the personal information should be irrelevant to consumer expectations. We agree, however, that the degree of a third party's involvement is a relevant factor when determining whether processing is consistent with a consumer's reasonable expectations given that third parties are not similarly bound to the business's determination of the purposes and means of processing personal information.

Accordingly, we recommend that the Agency strike the references to service providers and contractors in Section 7002(b)(5) so as to resolve the concern noted above, as well as to prevent the possible unintended effect of discouraging the use of service providers and contractors.

*Proposed Amendments:*

Sec. 7002(b): "(5) The degree to which the involvement of ~~service providers, contractors,~~ third parties, ~~or other entities~~ in the collecting or processing of personal information is apparent to the consumer(s). ~~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.~~"

**2. Working With Service Providers, Contractors, and Third Parties (Sec. 7051 and 7053)**

**A. Requirements for Agreements with Service Providers, Contractors, and Third Parties (Sec. 7051(a)-(c) and 7053)**

We respectfully suggest that the Agency take further action to ensure that the final regulations do not impose lengthy, prescriptive requirements for contracts with services providers, contractors, and third parties. While the modified proposed regulations helpfully remove a few of these requirements, many provisions remain that would impose new, substantive requirements for agreements, beyond those imposed by the CPRA, such as the specificity with which contracting entities must disclose the "Business Purposes" of the processing. Moreover, the modified proposed

Brian Soublet  
November 21, 2022  
Page 3

regulations continue to impose substantial unnecessary risk on companies' practices given that even immaterial non-compliance with a single contractual requirement potentially exposes businesses to significant penalties even where there is no conceivable consumer harm.

We ask that the Agency reconsider the proposed changes that we suggested in our prior letter—to strike the requirements set forth in Sections 7051(a)-(c) and 7053, or, alternatively, to include a materiality standard such that companies would not be punished for trivial violations or immaterial non-compliance. Such changes are necessary to ensure that the regulations do not impose stringent, overly prescriptive requirements for contracts with service providers, contractors, and third parties.

*Proposed Amendments:*

We propose that the Agency strike Section 7051(a)-(b). Alternatively, we propose that the Agency edit Section 7050(e) and 7052(a) as follows:

Sec. 7050(e): “A person who does not have a contract that complies **in material respects** with section 7051, subsection (a), is not a service provider or a contractor under the CCPA. For example, a business’s disclosure of personal information to a person who does not have a contract that complies **in material respects** with section 7051, subsection (a) may be considered a sale or sharing of personal information for which the business must provide the consumer with the right to opt-out of sale/sharing.”

7052(a): “A third party that does not have a contract that complies **in material respects** with section 7053, subsection (a), shall not collect, use, process, retain, sell, or share the personal information that the business made available to it.”

**B. Businesses’ Required Due Diligence of Service Providers and Contractors  
(Sec. 7051(c))**

The modified proposed regulations continue to contemplate imposing potential liability on businesses for the acts of the counterparties with whom they contract. Specifically, under Section 7051(c) (previously, Section 7051(e)), businesses could be deemed to have knowingly provided personal information to a service provider who the business knew would use such information in violation of the law, merely by disclosing the personal information without having tested such provider’s systems, even if the disclosure was made pursuant to a contract in compliance with the CCPA and the regulations. This, in combination with the numerous substantive requirements for contracts with service providers and contractors, unjustifiably exposes businesses to possible liability for the actions of its service providers irrespective of whether the business is substantively in full compliance with the law. Moreover, Section 7051(c) undermines the CPRA’s own standard

Brian Soublet  
 November 21, 2022  
 Page 4

of liability regarding disclosures to service providers and contractors, which requires “actual knowledge, or reason to believe, that the service provider or contractor intends to” violate the law.<sup>1</sup> Thus, we urge the Agency to reconsider the proposed changes that we put forth in our prior letter reiterated again below.

*Proposed Amendment:*

Sec. 7051(c): ~~“Whether a business conducts due diligence of its service providers and contractors factors into whether the business has reason to believe that a service provider or contractor is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract nor exercises its rights to audit or test the service provider’s or contractor’s systems might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the service provider or contractor.”~~

**3. Agency Audits (Sec. 7304)**

The Agency has made no revisions to the auditing provision in Section 7304. We urge the Agency to reconsider that the scope of audits should be limited to the provision(s) alleged to have been violated by the business and confirm that audits will be confidential. Anchoring audits in this manner would maximize the Agency’s effectiveness of audits that benefit consumers while also minimizing the compliance burden on businesses. Thus, we urge the Agency to reconsider the proposed changes we put forth in our prior letter, including the specific redlines we propose again below.

*Proposed Amendments:*

Sec. 7304: “(a) Scope. The Agency may audit a business’s ~~existing books, papers, or records, service provider, contractor, or person~~ to ensure compliance with any provision of the CCPA. ~~The scope of the audit shall be limited to the CCPA provision that the Agency reasonably suspects is being violated, and shall be limited to a time frame reasonably necessary to audit the suspected violation.~~

(b) Criteria for Selection. The Agency may conduct an audit ~~to investigate possible violations of where the Chief Privacy Officer finds reasonable suspicion that a business is violating a provision of the CCPA. Alternatively, the Agency may conduct an audit if the subject’s collection or~~

---

<sup>1</sup> See CPRA § 1798.145(i).

Brian Soublet  
 November 21, 2022  
 Page 5

~~processing of personal information presents significant risk to consumer privacy or security, or if the subject has a history of noncompliance with the CCPA or any other privacy protection law.~~

(c) Audits must be announced ~~to the business or unannounced as determined~~ by the Agency in writing with thirty days' notice. Such notice shall identify the provision of the CCPA that serves as the basis for the audit; describe the suspected violation; identify the books, papers, or records the Agency intends to review; and provide the date and time of the audit.

(d) Failure to Cooperate. A subject's failure to cooperate during the Agency's audit may result in the Agency issuing a subpoena ~~for the books, papers, or records at issue, seeking a warrant, or otherwise exercising its powers to ensure compliance with the CCPA.~~

(e) Protection of Personal Information. ~~The Agency shall not seek disclosure of consumer personal information during an audit in the absence of a court order, warrant or subpoena. Consumer personal information disclosed to the Agency during an audit shall be maintained in compliance with the Information Practices Act of 1977, Civil Code section 1798, et seq. Audits shall be confidential. At the conclusion of the audit, the audited party may request the destruction or return of any materials provided by the audited party."~~

#### **4. Enforcement (Sec. 7301 - 7303)**

##### **A. Investigations (Sec. 7301)**

In our prior comments, we urged the Agency to include provisions on investigations that align with the CPRA's mandate that the Agency may investigate "possible violations" of the law.<sup>2</sup> Accordingly, we asked that, at a minimum, the Agency be required to have a reasonable suspicion that a business has violated the law in order to initiate investigations. The modified proposed regulations clarify that the Agency may initiate investigations on its own initiative.<sup>3</sup> However, absent language clarifying the circumstances or criteria under which the Agency must operate to initiate investigations on its own, such investigations threaten due process rights. Thus, we ask that the Agency reconsider our prior comments on imposing a "reasonable suspicion" standard for initiating investigations to better align the regulations with the text of the CPRA and ensure that the Agency focuses its efforts on instances where a violation may exist. We urge the Agency to reconsider the proposed changes we put forth in our prior letter, including the specific redlines we reiterate again below.

---

<sup>2</sup> *Id.* § 1798.199.45.

<sup>3</sup> Modified Proposed Regulations § 7301(a).

Brian Soublet  
 November 21, 2022  
 Page 6

*Proposed Amendment:*

Sec. 7301: “(a) The Agency may initiate investigations from referrals from government agencies or private organizations, and sworn, nonsworn, or anonymous complaints, or on the Agency’s own initiative, **but only where the Board, by a majority vote, finds reasonable suspicion that a business has violated the CCPA.**”

**B. Probable Cause Proceedings (Sec. 7302)**

The Agency has made only modest, non-substantive revisions to the provisions in Section 7302. We urge the Agency to reconsider the proposed changes we put forth in our prior letter, including our proposed redlines reiterated again below.

*Proposed Amendments:*

Sec. 7302: “(b) Probable Cause Notice. The Enforcement Division will provide the alleged violator with notice of the probable cause proceeding as required by Civil Code section 1798.199.50. **Such notice shall contain a clear statement of each claim against the alleged violator and a summary of the evidence in support of each such claim, as well as the documents and other evidence on which the Enforcement Division Staff will rely at the proceeding.**

(c) Probable Cause Proceeding. (1) The proceeding shall be closed to the public unless the alleged violator files, at least 10 business days before the proceeding, a written request for a public proceeding. If the proceeding is not open to the public, then the proceeding, **at the election of the alleged violator,** may be conducted in whole or in part by telephone or videoconference.

(d) Probable Cause Determination. The Agency shall issue a written decision with its probable cause determination and serve it on the alleged violator electronically or by mail. The Agency’s probable cause determination is final **for the purpose of determining that the Agency may hold an administrative hearing to determine whether there has been a violation of the CCPA under Cal. Civ. Code § 1798.199.55** and not subject to appeal. **If probable cause is not found, the Agency shall, at the alleged violator’s request, destroy or return any materials provided by the alleged violator.**

(e) Notices of probable cause, **information or arguments presented at the probable cause proceeding by the parties,** and probable cause determinations shall not be open to the public nor admissible in evidence in any action or special proceeding other than one enforcing the CCPA.”

**5. Technical Specifications for Opt-Out Preference Signals (Sec. 7025(b))**

Brian Soublet  
November 21, 2022  
Page 7

In our prior comments, we asked the Agency to act on its statutory mandate to define the requirements and technical specifications for an opt-out preference signal in accordance with the factors set forth in the CPRA. Respectfully, the modified proposed regulations still do not meet the Agency’s obligation to “define the requirements and technical specifications for 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 and to limit the use or disclosure of the consumer’s sensitive personal information,”<sup>4</sup> nor do they provide guidance on how the choice must be presented, such as to ensure that the opt-out preference signal is consumer-friendly, clearly represents a consumer’s intent, and does not conflict with other settings.<sup>5</sup> The insertion of “JavaScript object” as another example of a “commonly used and recognized” format for opt-out preference signals,<sup>6</sup> like the pre-existing example of an “HTTP header field”— are insufficient to provide businesses with clarity regarding how to look for and honor opt-out preference signals.

Absent the technical specifications called for by the CPRA, nor a process for the Agency to approve proposed signals, the concept of automated opt-out signals cannot serve their intended purpose of empowering consumers to opt out in a seamless and predictable manner. To do so, businesses must know what signals to look for and how to process them. Thus, per our prior comments, we urge the agency to provide clarity on what signals are valid under the law and how companies are to respond to them at a technical level. In particular, the Agency should tell businesses which particular signals, formats, or tools are valid. In doing so, the Agency should adopt an approach that is similar to the draft regulations implementing the Colorado Privacy Act (“Draft Rules”), which require the Colorado Department of Law to maintain a public list of Universal Opt-Out Mechanisms. This model would be a step to help provide clarity as to which signals must be honored. The Agency should also, similar to the Draft Rules, state with greater precision the criteria that make a signal, format, or tool qualify under the law.

*Proposed Amendment:*

We propose that the Agency strike Section 7025 of the proposed regulations in its entirety until the Agency defines the requirements and technical specifications for opt-out preference signals.

\*\*\*\*\*

---

<sup>4</sup> See CPRA § 1798.185(a)(19)(A).

<sup>5</sup> *Id.* § 1798.185(a)(19)(A)(i)-(vi).

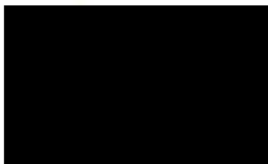
<sup>6</sup> See Modified Proposed Regulations § 7025(b)(1).



Brian Soublet  
November 21, 2022  
Page 8

We appreciate the Agency's work on the CPRA regulations, and we appreciate the opportunity to provide these comments on the proposed regulations.

Sincerely,



James G. Snell

JGS:rs

---

**From:** David Reid [REDACTED]  
**Sent:** Monday, November 21, 2022 5:18 PM  
**To:** Regulations  
**Subject:** CCPA Public Comment - Receivables Management Association International  
**Attachments:** RMAI Comments to CCPA Modified Text of Proposed Regulations 11-21-2022.pdf

**WARNING:** This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear CCPA:

On behalf of RMAI Executive Director Jan Stieger, the Receivables Management Association International appreciates this opportunity to submit the attached comments in response to the Notice of Modifications to Text of Proposed Regulations dated November 3, 2022.

Thank you, and please let us know if you have any questions.

Sincerely,

David Reid

**David E. Reid**   
General Counsel



1050 Fulton Avenue, Suite 120

Sacramento, CA 95825

Office: [REDACTED]

Direct: [REDACTED]

Cell: [REDACTED]

[Linked in profile](#)

**About the Receivables Management Association International** – The Receivables Management Association International (RMAI) is a nonprofit trade association that represents the Receivables Management Industry. RMAI’s [Receivables Management Certification Program](#) and [Code of Ethics](#) protect consumers and businesses by setting the gold standard through uniform industry best practices. RMAI provides networking, education, and business development opportunities through events and communications. RMAI also maintains a highly effective grassroots advocacy program at the state and federal levels. Founded in 1997, RMAI is headquartered in Sacramento, California.

November 21, 2022

California Privacy Protection Agency  
Attn: Brian Soublet  
2010 Arena Blvd.  
Sacramento, CA 95834

Sent via email: [regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

Re: RMAI Comments on CCPA Modified Text of Proposed Regulations

Dear Mr. Soublet:

The Receivables Management Association International (“RMAI”) appreciates this opportunity to submit the following comments to the California Privacy Protection Agency (“Agency”) regarding the Modified Text of Proposed Regulations relating to the California Consumer Privacy Act of 2018 (“CCPA”) and California Privacy Rights Act (“CPRA”).

### I. BACKGROUND

RMAI is the nonprofit trade association that represents more than 590 companies that purchase or support the purchase of performing and non-performing receivables on the secondary market. The existence of the secondary market is critical to the functioning of the primary market in which credit originators extend credit to consumers. An efficient secondary market lowers the cost of credit extended to consumers and increases the availability and diversity of such credit.

RMAI is an international leader in promoting strong and ethical business practices within the receivables management industry. RMAI requires all its member companies who are purchasing receivables on the secondary market to become certified through RMAI’s Receivables Management Certification Program (“RMCP”)<sup>1</sup> as a requisite for membership. The RMCP is a comprehensive and uniform source of industry standards that has been recognized by the collection industry’s federal regulator, the Bureau of Consumer Financial Protection, as “best practices.”<sup>2</sup>

RMAI supports the adoption of reasonable measures designed to protect consumer privacy. With respect to data security, RMCP certified companies are required to establish and maintain a reasonable and appropriate data security policy that includes, at a minimum, measures to ensure:

- (a) The safe and secure storage of physical and electronic Consumer Data;

<sup>1</sup> RMAI, *RMAI Receivables Management Certification Program*, <https://rmaassociation.org/certification> (last accessed November 18, 2022).

<sup>2</sup> Consumer Financial Protection Bureau, *Small Business Review Panel for Debt Collector and Debt Buyer Rulemaking, Outline of Proposals Under Consideration*, July 28, 2016, p. 38, [http://files.consumerfinance.gov/f/documents/20160727\\_cfpb\\_Outline\\_of\\_proposals.pdf](http://files.consumerfinance.gov/f/documents/20160727_cfpb_Outline_of_proposals.pdf) (last accessed November 18, 2022).

(b) Computers and other electronic devices that have access to Consumer Data contain reasonable security measures such as updated antivirus software and firewalls;

(c) Receivables portfolios are not advertised or marketed in such a manner that would allow Consumer Data and Original Account Level Documentation to be available to or accessible by the public;

(d) If there is any offsite access to a Certified Company's network, the offsite access shall be through the use of a virtual private network "VPN" or other system that requires usernames and passwords, complex and non-intuitive passwords, recurring password changes, and multifactor authentication;

(e) The Certified Company can prevent connectivity with the network and/or remotely disable or wipe company-issued computers and electronic devices that contain Consumer Data when an employee or agent no longer has an employment/agency relationship with the company or if a device is lost or stolen;

(f) Consumer Data that is transferred to a third-party is transferred securely through the use of encryption or other secure transmission sources;

(g) An action plan has been developed and communicated with relevant employees on how to handle a data breach in accordance with applicable laws, which shall include any required disclosures of such breach;

(h) A disaster recovery plan has been developed and communicated with relevant employees on how to respond to emergencies (e.g., fire, natural disaster, etc.) that have the potential to impact the use and storage of data; and

(i) The secure and timely disposal of Consumer Data that complies with applicable laws and contractual requirements, provided that account records are maintained for at least three (3) years from the date of last collection activity.<sup>3</sup>

## II. COMMENTS

### Article 1. General Provisions.

#### § 7001. Definitions.

§ 7001(i). "Disproportionate Effort." RMAI appreciates the Agency's attempt to provide greater clarity around this term that appears in Civil Code §§ 1798.105, 1798.130, and 1798.185.<sup>4</sup>

<sup>3</sup> RMAI Certification Standard A7, v10.

<sup>4</sup> ISR, p. 4.

Nevertheless, in many situations it will be a difficult compliance task for businesses to draft specific “adequate processes and procedures” to make disproportionate effort determinations. The several examples provided by the Agency are helpful, but do not portray particularly close calls, which is where the problems will occur. The scale is not weighing “apples to apples,” but is instead weighing potential business resources against the highly speculative “reasonably foreseeable impact” to the consumer.

RMAI respectfully suggests that since the failure to “put in place adequate processes and procedures” negates the ability to assert that a request involves disproportionate effort, more guidance be provided as to specific “processes and procedures” that would be considered “adequate.”

§ 7001(kk). “Unstructured.” RMAI appreciates the proposed modification to this term, subject to the concerns discussed above regarding the term “disproportionate effort.”

### **§ 7002. Restrictions on the Collection and Use of Personal Information.**

§ 7002(a). RMAI appreciates that the term “average consumer” has been removed from this section as RMAI previously suggested, as well as from other sections, though the term still appears in §§ 7027(a) and 7027(m)(1).

§ 7002(d). RMAI appreciates the useful examples provided to aid in understanding the application of the proposed regulations. However, what is “reasonably necessary and proportionate to achieve the purpose” is subjective and therefore difficult to address with policies and procedures.

Additionally, subsection (d)(1) refers to the “minimum personal information that is necessary,” which is different from what is “reasonably necessary and proportionate.” “Minimum” refers an absolute lowest quantity, while a “reasonable” standard allows some flexibility.

Subsection (d)(2) requires consideration of the “possible negative impacts on consumers,” and subsection (d)(3) requires the use of “safeguards” to address such impacts. While the several examples provided are helpful, they are also clear cut. RMAI suggests more guidance and specificity should be provided on implementation of these concepts, which are not addressed in this context in the CCPA and arguably exceed statutory authority.

§ 7002(e). RMAI appreciates the Agency’s removal of the references to “explicit” consent.

§ 7002(f). The previous subdivision (e) requires a consumer to opt in before the business collects or processes personal information for purposes inconsistent with the consumer’s reasonable expectations. However, this subdivision, (f), requires a business to provide a new notice at collection if it intends to collect such information. Though not directly contradictory, the subdivisions raise the question as to what, exactly, a business must do prior to collecting this potentially incompatible personal information: 1) obtain consent; or 2) send a new Notice at

Collection; 3) both; or, 4) something else. RMAI suggests the Agency provide some guidance for reconciling these subdivisions.

---

**§ 7004. Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent.**

§ 7004(a)(2). California Civil Code § 1798.185(a)(4)(A) requires the adoption of rules that, among other things, “ensure that consumers have the ability to exercise their choices without undue burden.” To that end, RMAI appreciates that a symmetry standard that requires exactly the same number of steps to opt in as to opt out makes for easy enforcement. Nevertheless, it is entirely conceivable that to effectuate a “more privacy-protective option,” a business may develop a path that has more steps but does not present an undue burden.

§ 7004(c). RMAI appreciates the modification to this section that now allows a business’s intent to be “a factor to be considered” in dark pattern determinations. RMAI recommends the Agency describe in detail the types of evidence it anticipates examining to determine a business’s intent.

---

**Article 2. Required Disclosures to Consumers.**

**§ 7011. Privacy Policy.**

§ 7011(c)(2). This subpart requires that a business’s privacy policy notify consumers of their rights under the CCPA. However, many businesses only process personal information that is exempt from the CCPA pursuant to Cal. Civ. Code §1798.145. Accordingly, requests received will be denied with explanation, pursuant to §§ 7022(f)(1), 7923(f)(1), and 7024(e).

Informing consumers of their rights knowing that certain requests will be denied harms consumers by setting false expectations and wasting their time. Accordingly, RMAI suggests that the Agency clarify that neither the CCPA nor its regulations prohibit a business from explaining in its privacy policy that because all the personal information collected, processed, sold, or disclosed by the entity is exempt, consumers’ requests to exercise their rights under the CCPA may be denied.

---

**§ 7015. Alternative Opt-Out Link.**

RMAI appreciates the Agency’s allowance of, and guidance regarding, the Alternative Opt-Out Link.

---

**Article 3. Business Practices for Handling Consumer Requests**

**§ 7020 Methods for Submitting Requests to Delete, Requests to Correct and Requests to Know.**

**§ 7020(b).** Businesses that operate only informational websites should not be required to accept requests to dispute or know using a webform. A survey conducted of RMAI members revealed that twenty percent (20%) operate websites that are not designed to collect information from or otherwise interact with consumers. These websites are designed as online brochures and are primarily used to advertise to the credit and collection industry. They do not engage consumers. Because the proposed regulation would apply to any business that “maintains an internet website,” regardless of whether the website collects information of consumers, it imposes an unnecessary burden.

Existing and proposed subsection (c) contemplates this very situation, noting:

A business shall consider the methods by which it interacts with consumers when determining which methods to provide for submitting requests to delete, requests to correct and requests to know ~~and requests to delete~~.

Thus, where a business does not use a website to interact with consumers, it should not be required to provide a webform to receive requests.

One important reason not to require “webforms” and similar web-based communications channels is to protect consumer privacy. The use of web-forms as an exploit by bad actors has exploded over the past two years. In a 2020 survey published by Cybersecurity Insiders, web server exploits were identified as a “most dangerous” malware attack vector by surveyed cybersecurity professionals.<sup>5</sup> Those same surveyed cybersecurity professionals pointed to customer information and financial data as the data “most at risk” to such exploits.<sup>6</sup>

The use of webforms to exploit sensitive non-public, private information is well documented. In 2008, criminals obtained 100 million debit and credit card numbers through a “SQL injection” into a webform on the website of Heartland Payment Systems.<sup>7</sup> In 2017, the Equifax data breach began through an exploit of its consumer complaint web portal.<sup>8</sup>

A business should exercise reasonable and appropriate measures to address data security. One measure to protect against the very type of exploit identified in the Equifax is to simply not allow

---

<sup>5</sup> Cybersecurity Insiders, *2020 Malware and Ransomware Report*, p. 10, publicly available at <https://static.helpsystems.com/core-security/pdfs/reports/cts-2020-malware-report-coresecurity.pdf> and archived at <https://perma.cc/UPC2-4KKU>.

<sup>6</sup> *Id.*, p. 8.

<sup>7</sup> *Heartland Payment Systems: Lessons Learned from a Data Breach*, Cheney, Julia S., Federal Reserve bank of Philadelphia, Payment Cards Center, (Jan 2010), pp. 2-3. Publicly available at <https://www.philadelphiafed.org/-/media/frbp/assets/consumer-finance/discussion-papers/D-2010-January-Heartland-Payment-Systems.pdf> and archived at <https://perma.cc/WB7J-VCLN>.

<sup>8</sup> *Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach*, United States Government Accountability Office, Report to Congressional Requestors, (GAO-18-559 Data Protection) (Aug. 2018), p. 10 (“The breach of an Equifax online dispute portal from May to July 2017 resulted in the compromise of records containing the PII of at least 145.5 million consumers in the U.S. and nearly 1 million consumers outside of the U.S.”). Publicly available at <https://www.warren.senate.gov/imo/media/doc/2018.09.06%20GAO%20Equifax%20report.pdf> and archived at <https://perma.cc/8ZMV-JQAB>.

consumers “methods for submitting these requests . . . through its website.” In fact, as recent as August 11, 2022, the Consumer Financial Protection Bureau issued a circular explaining that in the case of the Equifax breach, Equifax’s use of the unsecured webform portal to collect consumer complaints violated the federal Consumer Financial Protection Act’s prohibition against unfair acts and practices.<sup>9</sup> (“Equifax violated the prohibition on unfairness. . . by using software that contained a known vulnerability and failing to patch the vulnerability for more than four months. Hackers exploited the vulnerability to steal over 140 million names, dates of birth, and SSNs, as well as millions of telephone numbers, email addresses, and physical addresses, and hundreds of thousands of credit card numbers and expiration dates.”). To address such vulnerabilities, companies are expected to “routinely update systems, software, and code (including those utilized by contractors).”<sup>10</sup>

As a result, a business may reasonably choose to secure consumer data by not using webforms or accepting non-public personal information through a web portal. A regulation designed to protect consumer privacy should not require the use of platforms proven, time and again, to have compromised the private data of millions of Americans. The proposed amendment creates an unacceptable risk for both covered entities and consumers. To be sure, even if a covered entity was to accept documents and data through a secure and carefully protected webform, consumers are still at risk. The Federal Bureau of Investigation reports that “spoofing” of website domains has become a common means by which cybercriminals obtain consumer information.<sup>11</sup> “Spoofed” domains are websites made to appear like a trusted website, usually by making a slight alteration to a known URL. To be sure, the FBI identified its own domain as subject to potential spoofing.<sup>12</sup>

**§ 7020(f) (Proposed).** Requiring businesses subject to the federal Fair Debt Collection Practices Act (“FDCPA”), 15 USC § 1692, *et seq*, to notify consumers of their rights to know, correct, or delete, will confuse consumers.

Businesses, including most RMAI members, that are subject to the FDCPA are required to notify consumers of the right to obtain “verification” of a debt. 15 USC § 1692g(a). A consumer can obtain verification by contacting the debt collector “in writing.” RMAI believes that requests to know and requests to correct could be seen as synonymous with a request for verification under the FDCPA, as they are requests for information the debt collector has concerning the consumer.<sup>13</sup> It is likely that a consumer will believe that by submitting a request to know or request to correct using a 1-800 telephone number or a webform, they have exercised their

<sup>9</sup> “Insufficient data protection or security for sensitive consumer information,” Consumer Financial Protection Bureau Circular 2022-04 (Aug. 11, 2022), p. 4, publicly available at [https://files.consumerfinance.gov/f/documents/cfbp\\_2022-04\\_circular\\_2022-08.pdf](https://files.consumerfinance.gov/f/documents/cfbp_2022-04_circular_2022-08.pdf) and archived at <https://perma.cc/3TEH-6YT4>.

<sup>10</sup> *Id.*, p. 7.

<sup>11</sup> *Spoofed FBI Internet Domains Pose Cyber and Disinformation Risks*, Federal Bureau of Investigation, Alert No. I-112320-PSA (Nov. 23, 2020) publicly available at <https://www.ic3.gov/Media/Y2020/PSA201123> and archived at <https://perma.cc/7GBQ-LLAY>.

<sup>12</sup> *Id.*

<sup>13</sup> See, 15 U.S.C. § 1692g.



validation rights under the FDCPA. This would not be the case since neither communication was made “in writing.”<sup>14</sup>

Additionally, RMAI believes that a consumer is likely to believe that a request to delete is synonymous with a demand to cease communications under § 1692c(c), which provides:

If a consumer notifies a debt collector in writing that the consumer refuses to pay a debt or that the consumer wishes the debt collector to cease further communication with the consumer, the debt collector shall not communicate further with the consumer with respect to such debt . . .

In fact, out of an abundance of caution and for the purpose of mitigating risk, a business subject to the FDCPA may treat a request to delete as a demand to cease communication under § 1692c(c), if the request is made in writing.

RMAI believes that flexibility is needed in determining the best means to allow consumers to make the requests in a manner that does not lead to confusing consumers of their rights under other law. Therefore, RMAI requests that the final rule reflects that a business subject to the FDCPA may choose “one or more methods” which are reflective of their usual interaction with consumers. Therefore, RMAI proposes the addition of § 7020(f):

A business that is a “debt collector” as defined by 15 U.S.C. § 1692a(6) shall only be required to provide an email address, mailing address or other means of electronic communication reflective of their usual interaction with consumers, for submitting requests to delete, requests to correct, and requests to know.

In this way, businesses subject to the FDCPA may define the channels of consumer communication that avoid consumer confusion and promote compliance with both the CCPA and other law.

---

## **§ 7022. Requests to Delete.**

**§ 7022(b)(3).** RMAI suggests that the Agency provide guidance and examples regarding the “detailed explanation” that must be provided to consumers.

**§ 7022(c)(4).** The triggering event of proposed § 7022(c)(4) is not connected to the consumer requesting deletion. Section 7022(c)(4) proposes that certain service providers must be notified to delete the consumer’s personal information if “they may have accessed personal information from or through the service provider or contractor . . .” RMAI believes that what was intended as the trigger event is that the covered service provider *has* accessed the *requesting consumer’s* personal information. As proposed, such a notice must be provided even if the service provider

---

<sup>14</sup> See, *Mahon v. Credit Bureau, Inc.*, 171 F.3d 1197, 1202 (9th Cir. 1999) (“If no written demand is made, ‘the collector may assume the debt to be valid,’” citing *Avila v. Rubin*, 84 F.3d 222, 226 (7th Cir. 1996); 15 U.S.C. § 1692g(a)(3)).

never accessed the requesting consumer's information, but *may* have accessed the personal information of other consumers. Therefore, RMAI, proposes the following:

Notifying any other service providers, contractors, or third parties that **may** have accessed the consumer's personal information from or through the service provider or contractor, unless the information was accessed at the direction of the business, to delete the consumer's personal information unless this proves impossible or involves disproportionate effort.

### **§ 7025. Opt-Out Preference Signals.**

Subdivision (a) of Cal. Civ. Code § 1798.135<sup>15</sup> provides that a business may either: 1) provide “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links; or 2) use what is referred to in the regulations as the Alternative Opt-Out Link.

On the other hand, § 1798.135(b)(1) provides a business need not provide the links described in subdivision (a) *if* the business allows consumers to opt out using an opt-out preference signal. Paragraph (b)(2) begins: “A business *that allows* consumers to opt out . . . pursuant to [an opt-out preference signal] . . .” Clearly, this anticipates businesses that, on the other hand, don't allow opt out through the use of opt-out preference signals. In fact, paragraph (b)(3) states:

A business that complies with subdivision (a) is not required to comply with subdivision (b). For the purposes of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b).

Nevertheless, the Agency asserts in § 7025(e) that the statute “does not give the business the choice between posting the above-referenced links or honoring opt-out preference signals. Even if the business posts the above-referenced links, the business must still process opt-out preference signals . . .” This position appears to directly contradict Cal Civ. Code § 1798.135(b), and particularly paragraph (b)(3).

## **Article 4. Service Providers, Contractors, and Third Parties**

### **§ 7051. Contract Requirements for Service Providers and Contractors.**

**§ 7051(a)(7).** RMAI suggests that the phrase “in a manner consistent with the business's obligations under the CCPA and these regulations” could be more precise and helpful by citing to, or describing with more detail, those specific obligations.

### **§ 7304. Agency Audits.**

<sup>15</sup> Effective January 1, 2023.

§ 7304(b). RMAI suggests the Agency define the specific criteria it will use to determine whether processing presents “significant risk.”

§ 7304(c). RMAI respectfully disagrees with the concept of unannounced audits. Audits typically require the dedication of significant resources on the part of a business and, without prior announcement, could seriously disrupt the ability of a business to provide goods or services to consumers. RMAI suggests that if this option is to be exercised at all, it be limited to businesses that have been found to have violated the CCPA and are subject to continuing supervision.

---

### III. CONCLUSION

RMAI thanks the California Privacy Protection Agency for its many thoughtful modifications to the proposed rules and for its consideration of these comments.

If you have any questions or if we can be of any assistance, please contact RMAI General Counsel David Reid at [REDACTED]

Sincerely,

[REDACTED]

Jan Stieger  
RMAI Executive Director