



Consumer Data Industry Association 1090  
Vermont Ave., NW, Suite 200  
Washington, D.C. 20005-4905

P 202 371 0910

Writer's direct dial: +1 (202) 408-7407

[CDIAONLINE.ORG](http://CDIAONLINE.ORG)

November 20, 2022

***Via Electronic Delivery to***  
***[regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)***

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

**RE: CPPA Public Comment in response to Notice of Modifications to Text of Proposed Regulations concerning the California Consumer Privacy Act**

Dear Mr. Soublet,

The Consumer Data Industry Association submits this comment letter in response to the California Privacy Protection Agency ("CPPA") Notice of Modifications to Text of Proposed Regulations on proposed changes to California Consumer Privacy Act ("CCPA") regulations related to the California Privacy Rights Act ("CPRA").

The Consumer Data Industry Association ("CDIA") is the voice of the consumer reporting industry, representing consumer reporting agencies including the nationwide credit bureaus, regional and specialized credit bureaus, background check and residential screening companies, and others. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals and to help businesses, governments, and volunteer organizations avoid fraud and manage risk. Through data and analytics, CDIA members empower economic opportunity all over the world, helping ensure fair and safe transactions for consumers, facilitating competition, and expanding consumers' access to financial and other products suited to their unique needs.

CDIA members have been complying with laws and regulations governing the consumer reporting industry for decades. Members have complied with the Fair Credit Reporting Act ("FCRA"), which has been called the original federal consumer privacy law. The FCRA governs the collection, assembly, and use of consumer report information and provides the framework for the U.S. credit reporting system. In particular, the FCRA outlines many consumer rights with respect to the use and accuracy of the information contained in consumer reports. Under the FCRA, consumer reports may be accessed only for permissible purposes, and a consumer has the right to dispute the accuracy of any information included in his or her consumer report with a consumer reporting agency ("CRA").

CDIA members have been at the forefront of consumer privacy protection. Fair, accurate, and permissioned use of consumer information is necessary for any CDIA member client to do business effectively.

CDIA appreciates the CPPA's invitation to comment on this important rulemaking process. CDIA also appreciates the CPPA's consideration of CDIA's previous comments, like on issues related to consumer disclosure font size and color, requests to know, and third party deletion requests. However, CDIA remains concerned with certain proposed sections and urges the CCPA to clearly provide that businesses may engage in purposes consistent with previous disclosures, businesses may retain information corrected by a consumer, businesses may retain sensitive personal information to prevent fraud, and service providers and contractors may sell or share personal information if the law otherwise permits it.

To assist the agency in finalizing clear and effective regulations that allow businesses to best support customers and consumers, CDIA offers the following comments on the proposed revisions:

## **I. Delaying Enforcement of New Rules**

As an initial matter, CDIA strongly encourages the CPPA to postpone enforcement of the CPRA until one year after regulations are finalized. The CPRA required the CPPA to finalize regulations by July 1, 2022, providing one year until enforcement would begin, on July 1, 2023. Further, September 2022 developments in the California legislature now require businesses to assess personal information for CCPA compliance previously exempted from the law.

Because the regulations were not finalized as provided for in the CPRA, enforcement should be postponed to one year after the regulations are finalized. In particular, CDIA strongly urges the CPPA to provide at proposed section 7301 that investigations may not be initiated until a year after regulations are finalized.

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

The CPRA, at Cal. Civ. Code § 1798.100(a)(1), provides that a “business shall not . . . use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected, without providing the consumer with notice consistent with this section.” Further, section 1798.100(c) provides that a “business’s collection [and] use . . . of a consumer’s personal information shall be reasonably necessary to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with these purposes.” Considering these two sections together, it is clear that a business can use personal information for the purpose it disclosed to the consumer at collection (limited to what is reasonably necessary and proportionate to achieve that purpose) or for a purpose *later*

disclosed to the consumer, so long as that later-disclosed purpose is not inconsistent with the first disclosed purpose.

Proposed section 7002(a) states that a business' collection, use, retention, and/or sharing of consumer personal information must be necessary and proportionate to achieve the purpose or purposes for which the personal information was collected or processed or another disclosed purpose that is compatible with the context in which the personal information was collected. The proposed section goes beyond the text of the statute and lays out a complex and confusing 5-factor formula to assess whether actual uses are reasonably necessary and proportionate, and then whether they are compatible, with consumer expectation, not the previous disclosures. In particular, it seems the CPPA is expressing a view on compatibility that is far narrower than what is reflected in the statute. While the drafted language is ambiguous, it may be the case that the CPPA may envision that later-disclosed but compatible purposes must be a Business Purpose listed in Cal. Civ. Code § 1798.140(e)(1) through (8), while a plain reading of the statute would lead one to believe that later-disclosed purposes are only impermissible when they contradict, undermine, or stand opposed to *the initially-disclosed purposes*.

What results from the ambiguity of the draft language is an excessive amount of discretion placed into the hands of the CPPA, more than the CPRA contemplates. The five factors ultimately provide no helpful guidance to businesses and create confusion and risk for businesses mapping out their processing uses. CDIA believes that the standards here should depend on disclosures and compatibility with prior disclosures, not on other factors not articulated by the CPRA under a consumer expectations umbrella.

CDIA encourages the CPPA to revisit this section to reflect the collection and use permissibility as articulated by the CPPA. CDIA welcomes guidance from the CPPA, but that guidance needs to be both clear and consistent with the law.

### **III. Requests to Delete**

Proposed section 7022(b) requires businesses to notify third parties to whom the business has sold or shared personal information of a consumer's request to delete personal information. However, the proposed rule includes no limitations on this notification requirement, such as limiting where the business sold or shared personal information within the previous year. CDIA strongly urges the CPPA to provide for reasonable limits so that businesses are not required to retain records of the personal data, transfers, and uses indefinitely simply to comply with this notification requirement.

### **IV. Requests to Correct**

Proposed section 7023 states, in part:

“(c) A business that complies with a consumer's request to correct shall correct the

personal information at issue on its existing systems.”

Businesses that retain information for the purpose of detecting and preventing fraud, identity theft, or security incidents need to be able to retain personal information in original form, despite any request to correct. For example, if a consumer contacts a business, verifies their identity, and updates their address, businesses need the flexibility to retain the former address for use in future identity verification needs, rather than being required to update it and delete the old information. Further, businesses need to be able to retain previously-collected personal information for other reasons, particularly complying with legal obligations (for example, legal holds), complying with contract obligations (for example, updating information through third-party sources like USPS address change notifications), processing the information for other limited internal uses not incompatible with previously disclosed purposes. This proposed section does not clearly permit businesses to retain information it updates as previous data points, and CDIA urges the CPPA to explicitly permit retention of personal information for the purposes already detailed in the CCPA for the right to delete, at Cal. Civ. Code § 1798.105(d).

Additionally, the proposed “totality of circumstances” test provides new and broader criteria for business to consider when determining whether to deny a consumer’s request to correct personal information. In particular, the proposed rule states that in the case that the business is not the original source of the personal information, “the consumer’s assertion of inaccuracy may be sufficient to establish that the personal information is inaccurate.” Under the proposed test, businesses would be required to accept, review, and consider any documentation that the consumer provides and explain the basis for denial to the consumer. This would prove challenging to businesses that do not have direct interaction with the consumer in question. These challenges would be particularly acute with regard to the requirement to provide a detailed explanation of the basis for the denial and could create confusion for consumers. CDIA thus respectfully requests that businesses be granted the option to treat a request to correct in the same manner as a request to delete.

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

Proposed section 7027(l)(3) permits businesses to use and disclose sensitive personal information in order to resist malicious, deceptive, fraudulent, or illegal actions directed at the business without requiring those businesses to offer consumers a right to limit. However, this exception does not clearly extend to a business’ efforts to prevent fraud or other malicious, deceptive, or illegal actions on other businesses. Conversely, the CPRA, at Civil Code, § 1798.121(a), provides for a broader exception, permitting the use and disclosure of sensitive personal information to help to ensure security and integrity. Cal. Civ. Code § 1798.140(e)(2).

CDIA members provide “security and integrity” services, like fraud detection and identity verification services, to their business customers. Providing these services may involve comparing inquiry data with data available elsewhere, detecting anomalies in provided data, and otherwise analyzing multiple data sets, all with the goal of detecting—and thus preventing—identity theft, fraud, and other illegal actions on businesses and consumers. These efforts reduce

business costs and protect consumers, whether such consumers are business customers or not, and thus further consumer privacy.

If fraud prevention services providers are unable even to use sensitive personal information to prevent fraud on third parties, consumer privacy may be affected significantly and detrimentally. CDIA strongly urges the CPPA to expand this exception to align with the CPRA and allow businesses to use sensitive personal information for fraud prevention and detection services related third parties to further consumer privacy and identity theft prevention efforts.

## **VI. Requests to Know or Delete Household Information**

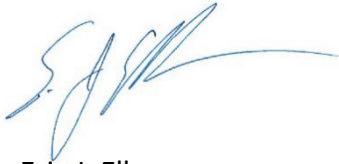
Section 7031 is proposed to be deleted in its entirety. This section provides for requirements under which consumers may provide requests with regard to household information, which is personal information under the CCPA. These requirements ensure that all members of the household agreed to such request, that the identity of all members would have to be verified, and that the members would have to be confirmed as current members of the household. Without this guidance, it is unclear how businesses would be expected to process household information requests, and whether businesses could deny such requests if they are unable to perform these reasonable checks to ensure the privacy of household members.

## **VII. Service Providers and Contractors and Contract Requirements**

Proposed section 7051(a)(1) restricts service providers from selling or sharing personal information they collect on behalf of the businesses to which they provide services. Other subsections impose other restrictions, including on retaining, using, or disclosing personal information other than those specified in the service provider agreement, “unless otherwise permitted by the CCPA and these regulations,” like subsection (a)(3). CDIA members provide fraud detection and prevention services and may do so, in some contexts, as a service provider to a business. Those services may involve the disclosure of personal information received on behalf of the business to third parties in relation to providing fraud detection and prevention services. CCPA regulations—notably proposed section 7050(a)(4)—specifically permit service providers to process data in their position to “prevent, detect, or investigate data security incidents or protect against malicious, deceptive, fraudulent, or illegal activity, even if this Business Purpose is not specified in the written contract required by the CCPA and these regulations.” In order to ensure that fraud prevention and detection service providers can continue to provide their important services related to minimizing identity theft and fraud on consumers and businesses, CDIA strongly urges the CPPA to add “unless otherwise permitted by the CCPA and these regulations” to subsection (a)(1), as it does with other contract requirements.

Thank you for the opportunity to share our views on the anticipated rulemaking under the CPRA. Please contact us if you have any questions or need further information based on comments.

Sincerely,

A handwritten signature in blue ink, appearing to read 'E. Ellman', with a long horizontal flourish extending to the right.

Eric J. Ellman

Senior Vice President, Public Policy & Legal Affairs