Articles + Publications | November 23, 2022

# Silver Lining for Cos. in Proposed Calif. Privacy Law Changes

**WRITTEN BY**

James Koenig | Kim Phan | Joel M. Lutz | Sadia Mirza | Robyn W. Lin

*Published in Law360 on November 23, 2022.* 

On Oct. 17 and again on Nov. 3, the California Privacy Protection Agency, or CPPA, modified the text of the proposed regulations implementing the California Privacy Rights Act, or CPRA.[1]

This modification kicked off a 15-day comment period during which the CPPA accepted written comments regarding the proposed changes and material added to the rulemaking file until Nov. 21.

The deadline for promulgating regulations as set out under the CPRA has long passed, which means businesses are eager to receive finalized rules.

Given that we are already more than halfway into November, and in light of the Office of Administrative Law's 30-day review period, the soonest companies will likely receive finalized regulations is at the end of January or February.

However, depending on what transpires during the comment period and the following activity, this timeline may be further delayed.

For a full overview of the changes made during this latest round of edits, businesses can view the chart made available by the CPPA.[2]

This article focuses on those changes that may make businesses more optimistic about their compliance strategies and provides thoughts on an approach given the year-end compliance deadline.

**Draft regulations may make it easier to respond to data subject requests: Complications of unstructured data continue to be highlighted.**

The initial draft of the proposed regulations defined "unstructured" as "personal information that is not organized in a predefined manner, such as text, video files, and audio files." The modified proposed regulations are to:

- Remove the examples reasoning that there may be some instances in which text, video files and audio files constitute structured data; but

- Add that unstructured data is that which cannot be retrieved or organized in a predefined manner without disproportionate effort on behalf of the business, service provider, contractor or third party.

So, what's a disproportionate effort? The CPPA is still deciding.

For now, and within the context of responding to a consumer's CCPA request, the modified proposed regulations describe disproportionate effort as instances when

the time and/or resources expended … to respond to the individualized request significantly outweighs the reasonably foreseeable impact to the consumer by not responding, taking into account applicable circumstances such as, the size of the business, service provider, contractor, or third party, the nature of the request, and the technical limitations affecting their ability to respond.

Interestingly, the term "unstructured" is only used in the modified proposed regulations in connection with requests to correct, but businesses should consider how unstructured data affects other CPRA compliance obligations as well.

For example, with respect to responding to requests to know specific pieces of personal information, searching for personal information in unstructured data is challenging and could, at times, feel impossible.

Indeed, unstructured data could live in email accounts, chat software — e.g., Microsoft Teams — freeform fields in software, customer service ticketing systems, etc.

Whether or not businesses are required to search unstructured data in response to a consumer's CCPA request could depend on various factors, including how such data is used — e.g., is it solely for legal or compliance purposes, or is the data further sold or shared?

Where businesses are claiming disproportionate effort, it may be wise to at least disclose that this type of data is collected and give the consumer further options to discuss if additional information is needed.

**Security and fraud prevention: Exemption strengthened under modified regulations.**

Under the initial draft of the proposed regulations, service providers were permitted to retain, use and disclose personal information collected on behalf of a business to "detect data security incidents or protect against malicious, deceptive, fraudulent, or illegal activity."

Given the focus on the written contract, however, many service providers were explicitly calling out fraud prevention as a permitted use of personal information pursuant to the contract.

This is not only important for companies that provide security services, such as anti-fraud, but also provides clarity for any businesses who have been negotiating back and forth about whether their data could be used by their service providers for security and fraud prevention.

The modified proposed regulations expand the existing fraud exemption by clarifying that service providers may use personal information collected on behalf of a business 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.

Despite this change, it would be prudent for businesses and service providers to call out fraud prevention in the written contract, especially if fraud prevention is the primary business purpose of the contract.

**The CPPA's heart is in the right place: Some implementation areas have been simplified.**

In addition to the modified text of the proposed regulations, the CPPA issued an explanation of modified text of proposed regulations.

This chart explains the proposed changes in response to comments received during the 45-day comment period. Based on this chart, several changes were made to simplify implementation at this time. Below we have captured a few changes that may achieve this goal.

***Modifications to the Notice at Collection***

This deleted the requirement that the business identifies the names of the third parties that control the collection of personal information within its notice at collection. This may mean the recent inclusion of specificity around advertising technology vendors may be lightened for U.S.-only companies.

Nevertheless, this type of disclosure may still be required in some jurisdictions outside the U.S.

***Information Stored on Archived Backups***

This added language to enable businesses, service providers and contractors to delay compliance with requests to correct, with respect to information stored on archived backup systems.

***Data Correction***

This deleted the requirement concerning the business making a consumer's written statement — about the accuracy of their personal information being contested by the consumer — available to any person to whom it discloses, shares or sells personal information.

It also added revised language to the right to correct to provide flexibility and discretion to the business regarding whether it will provide the consumer with the name of the source from which the business received the alleged inaccurate information.

***Consumers' Opt-Out Status***

It deleted the language regarding the business displaying the status of the consumer's choice to opt out of the selling or sharing of their personal information because this is not a requirement but an option for the business.

It revised language to make it optional — instead of mandatory — for businesses to provide a means by which the consumer can confirm that their request to opt out of sale and sharing, or their request to limit, has been processed.

***Added definition of "nonbusiness" expressly carves out government entities.***

While there was some uncertainty, it was largely understood that nonprofits were excluded from the scope of the CPRA, the proposed regulations added in a definition for a nonbusiness.

A nonbusiness is exactly what you would expect it to be, namely a person or entity that does not meet the definition of a business, as that term is defined by the CPRA.

The CPPA then, however, lists nonprofits and government entities as examples of nonbusinesses, explaining that these types of entities are not "organized or operated for the profit or financial benefit of its shareholders or other owners."

Does this definition come as a surprise to most companies? Probably not. What is interesting, however, is the impact this definition will have on third-party vendors that provide services to government entities and nonprofits — two types of unregulated entities.

Addressing this point directly, the proposed regulations provide that "whether an entity that provides services to a nonbusiness must comply with a consumer's CCPA request depends upon whether the entity [providing the service] is a 'business.'"

The key seems to be whether the entity also controls "the purposes and means of processing the personal information at issue." If the entity has such control over the personal information at issue, it may be viewed as a business with respect to that data.

If, however, the entity does not control the purposes and means of processing, the entity likely would have no obligation to comply with a consumer's CCPA request with respect to that data.

Any other conclusion would likely create an unintended loophole in the law that would allow unregulated data — i.e., that belonging to a nonprofit or government entity — to become regulated.

**Agency investigations: Giving businesses some grace.**

While the 73 pages of proposed modified regulations may feel overwhelming, there is some good news once you get to page 71. Section 7301(b) was introduced in the latest round of changes and provides that

[a]s 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.

What does this mean for businesses? It means companies should continue to make good faith efforts to comply with the law, even in the absence of finalized regulations.

It also emphasizes the importance of not letting perfection be the enemy of good. In today's world, the reality is that businesses are collecting a significant amount of data in various forms — structured, unstructured, deidentified, aggregated, sensitive, etc.

Given this complexity, it is easy to see how a business could miss the forest for the trees, focusing too much on the minute details that they lose sight of the big picture.

Where good faith efforts to comply with the law count, it would be prudent for businesses, at least even initially, to focus their efforts on:

- Identifying their core systems and assets processing personal information;
- Accounting for those processing activities when addressing the CPRA's requirements; and
- Introducing mitigating steps that would minimize the potential for consumer harm or regulatory scrutiny in the event of any known gaps in compliance.

Following this approach at least would give businesses a good story to tell should the regulators come knocking.

---

[1] For the latest version of the draft regulations, see https://cppa.ca.gov/regulations/pdf/20221102_mod_text.pdf.

[2] The CPPA published an explanation of changes, see https://cppa.ca.gov/meetings/materials/20221021_22_expmodtext.pdf.

**RELATED INDUSTRIES + PRACTICES**

- Data + Privacy
- Privacy + Cyber