Blogs
November 29, 2022
Perkins on Privacy

One Step Closer: California Privacy Protection Agency Reviews Comments for CCPA Regulations

Last week, the period for comments closed on the California Privacy Protection Agency's (CPPA) latest version of the draft implementing regulations for the California Privacy Rights Act (CPRA) amendments to the California Consumer Privacy Act (CCPA) (Revised Regs). The Revised Regs were first released with modifications and an Explanation of Modified Text of Proposed Regulations at the end of October. Shortly thereafter, the CPPA released the current version of the Revised Regs, which, compared to the initial draft regulations (Initial Draft Regs), include many substantive modifications to key compliance areas.

The Agency's release followed the Colorado attorney general's publication of the proposed Colorado Privacy Act (CPA) draft rules (Draft Rules), which we analyzed in a prior communication. The Revised Regs differ from the initial draft regulations and the Colorado draft rules in several key respects. Below we outline and analyze some of the key provisions of the Revised Regs.

Disproportionate Effort

The Revised Regs introduce a set of factors for evaluating whether responding to consumer requests would require "disproportionate effort," including the size of the responding entity, the nature of the request, and the technical limitations affecting the ability to respond. This addition offers clarity for businesses, service providers, and third parties seeking to determine the scenarios in which responding to consumer requests would qualify as "disproportionate effort."

Permitted Processing Purposes

The Revised Regs substantially modify the standard for permissible processing. For example, the Initial Draft Regs dictated a standard of permissibility based on what an "average consumer" would expect, whereas the Revised Regs replace that standard with a two-part test allowing businesses to process personal information if doing so is "reasonably necessary and proportionate to achieve" either (1) the purpose(s) for which the personal information was collected or processed, or (2) another disclosed purpose that is compatible with the context in which the personal information was collected. *See* § 7002(a). The Revised Regs go on to list factors for determining whether processing is "consistent with" a consumer's "reasonable expectations," and whether processing is deemed "compatible" with the context of collection. *See* § 7002(b), (c).

Downstream Processing of Consumer Rights Requests

In response to deletion requests, the Initial Draft Regs required businesses to notify all third parties to whom personal information was sold or shared of such requests and instruct them to delete personal information. Although the Revised Regs continue to require this, they remove provisions dictating precisely how third parties are to treat such requests. Instead, the Revised Regs state that the manner in which third parties treat passed-down requests shall be determined by the contract between the business and the third party. As written, these

modifications would allow more flexibility in the drafting of contracts between businesses and third parties, no longer requiring that third parties comply with passed-down requests "*in the same way*" as the business, so long as both parties treat requests in accordance with the CCPA.

Although businesses would still be required to pass on *deletion* requests to third parties, they would no longer be obligated to pass down opt-out requests to third parties, provided that there is not a delay in processing the consumer's opt out that results in data being sold *after* the consumer opts out but *before* the request is processed. As with deletion requests, this topic is now left to the contract governing the relationship between the business and the third party.

Notice at Collection

The Revised Regs introduce a somewhat confusing standard wherein third parties do not have an obligation to provide Notice at Collection on a first-party business's website. Rather, a first party's Notice at Collection may include information about the first and third parties' *collective* practices. Alternatively, a third party may provide Notice at Collection on its Homepage.

It is unclear how this collective notice would be provided or whether it means that first parties would ask the third parties with whom they operate for information to include in their notices. In any event, most third parties are likely to view this as a positive change, preferring to provide Notice at Collection on their own sites rather than through first-party sites.

Relatedly, the Revised Regs removed the obligation for first parties to list all third parties that collect personal information on their website.

Service Providers and Contractors

The Revised Regs clarify that service providers and contractors are entitled to use personal information collected pursuant to their contract with the business to build or improve the quality of the services being provided, even if such use is not expressly stated in the contract, so long as they are not using the personal information to perform services on behalf of another person. The Revised Regs similarly clarify that a service provider's or contractor's use of the personal information to "prevent, detect, and investigate security incidents" is a permitted business purpose even if it is not expressly included in the contract with the business. These modifications would provide flexibility in how service providers and contractors may use personal information collected for internal purposes and relieve entities from having to account for every possible secondary use of personal information in the underlying contract.

Additional Modifications

Opt-out preference signals. The Revised Regs add "JavaScript object" as another example of a "commonly used and recognized" format for opt-out preference signals (along with "HTTP header field"). However, as drafted, the regulations provide little context for evaluating what signals to look for and how to process them.

Sensitive Personal Information. The Revised Regs modify obligations with respect to the processing of sensitive personal information to clarify that certain obligations do not apply to sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer.

Contractual Requirements. The Revised Regs include minor updates to the requirements for agreements with service providers, contractors, and third parties:

- *Service Providers and Contractors:* The Revised Regs clarify that contractual obligations imposed on service providers and contractors only extend to personal information processed pursuant to the written contract with the business. Additional revisions include: (1) clarifying that assessments, audits, or other technical and operational testing of the service provider's system can occur either "internal[ly] or [via a] third-party," (2) removing the required time period (previously, five business days) by which a service provider or contractor must notify the business after determining that it can no longer meet its obligations under the CCPA or regulations, and (3) enabling service providers and contractors to utilize self-service methods that allow the business to comply with consumer requests directly regarding personal information that the service provider or contractor collected for the business.
- *Third Parties.* The Revised Regs clarify that the contractual obligations imposed on third parties extend to personal information that the business "makes available to the third party," as opposed to personal information "sold or disclosed" to the third party, or "received by" the third party. Additional revisions include: (1) removing the requirement for third parties to check for and comply with a consumer's opt-out preference signal, (2) clarifying that a business may require the third party to treat the personal information the business made available to it in the "same manner" that the business is obligated to treat it under the CCPA and regulations, and (3) removing the required time period (previously, five business days) by which a third party must notify the business after determining that it can no longer meet its obligations.

Dark Patterns. The Revised Regs largely maintain the substance of the Initial Draft Regs, leaving in place the broad examples of how specific user interfaces constitute "dark patterns." Minor updates include removing examples suggesting that an icon's relative prominence affects choice symmetry. The Revised Regs also add that more "difficult" or "time-consuming" consumer choice paths are asymmetrical in the same manner as "longer" paths to the more privacy-protective option.

Next Steps

The 15-day public comment period for the Revised Regs closed on November 21, 2022. The CPPA is now considering the comments received, including whether to adopt or further modify the Revised Regs at a future public meeting.

It is unclear whether the CPPA is contemplating further modifications to this set of proposed regulations, or whether they will now turn their focus to issues like risk assessments, cybersecurity audits, and automated decision-making technology.

Our Privacy & Security Law team will continue to monitor upcoming developments and collaborate with our clients to ensure their concerns are heard as the CPPA moves forward with the rulemaking process.

Authors

Miriam Farhi

Partner
MFarhi@perkinscoie.com 206.359.8195

Explore more in

Privacy & Security
Blog series

Perkins on Privacy

Perkins on Privacy keeps you informed about the latest developments in privacy and data security law. Our insights are provided by Perkins Coie's Privacy & Security practice, recognized by Chambers as a leading firm in the field.

View the blog