CPRA Update: California Privacy Rulemaking Process Begins

Laura Riposo VanDruff, Alexander I. Schneider, Alysa Z. Hutnik, Aaron J. Burstein

September 26, 2021

On September 22, the California Privacy Protection Agency (CPPA) issued an invitation for public comments as part of its first "preliminary" rulemaking activities. Established by the California Privacy Rights Act (CPRA) ballot initiative last November, the CPPA has the authority to write rules that address some of the most technical and controversial topics addressed in the CPRA.

The CPPA's rulemaking process kicks off a little more than a year after the Office of the California Attorney General's first set of final rules implementing the California Consumer Privacy Act (CCPA) went into effect. The Attorney General Office's approach to CCPA regulations focused primarily on developing a standardized approach to implementing core CCPA compliance concepts: notice, responses to and verification of consumer requests, the service provider definition and obligations, and non-discrimination standards. The CPRA puts thornier issues into play for rulemaking: assessing risks to consumer privacy, standards for using automated decisionmaking, limiting uses of sensitive personal information, and further defining what it means to "combine" consumer personal information. Given the challenge ahead, it is not surprising that the CPPA indicated that it is not interested in re-litigating old battles addressed in the CCPA regulations, stating it is "particularly interested in comments on new and undecided issues not already covered by the existing CCPA regulations." Here's a preview of key rulemaking topics under consideration at the CPPA:

- **Opt Out Rights** The CPRA expands consumers' rights related to their personal information held by businesses, including adding a new right to opt out of "sharing" of personal information for cross context behavioral advertising, and a new right to limit the use and disclosure of sensitive personal information. The CPPA requests comments on how to allow consumers to limit use of sensitive personal information, how to apply opt-out rights to certain minors, and how to enable consumers who have opted out to consent to uses of their personal information. The CPPA also requests comment on how to interpret certain exemptions to the right to limit use and disclosure of sensitive personal information.The CPPA also delves directly into a debate on global privacy controls, asking "what requirements and technical specifications should define an opt-out preference signal sent by a platform, technology, or mechanism."

- **Intentional Interaction Standard** Closely related to the CCPA's opt-out right, an important, broad exemption to a "sale" involves an "intentional interaction" in which a consumer demonstrates through an interaction that the consumer agrees to the transfer of their personal information to a third party. The CPPA solicits comment on whether it should further refine the definition of "intentionally interacts."

- **Risk Assessments** The CPPA has the authority to require businesses that engage in activities that present a significant risk to consumer privacy or security to perform regular cybersecurity audits and privacy risk assessments (similar to DPIAs required by GDPR and data protection assessments under Virginia's and Colorado's privacy laws – the VCDPA and ColoPA, respectively).The CPPA solicits comments on the meaning of "significant risk" and the types of requirements that should apply to these regular audits and assessments. The CPPA also asks whether activities deemed an undue risk should be restricted or prohibited.

- **Automated Decisionmaking** The CPPA solicits feedback on how it should implement its authority regarding automated decisionmaking technology, including how to define "automated decisionmaking," the types of disclosures that should be provided to consumers, and any rights to opt out. Like risk assessments, this concept could mimic existing EU law. Article 22 of the GDPR restricts automated processing that produces legal effects or has a similarly significant effect on the individual. The VCDPA and ColoPA import similar concepts through their provisions on "profiling." It remains to be seen whether the CPPA will interpret its automated decisionmaking authority consistent with GDPR, Colorado, and Virginia.

- **Service Provider Restrictions on Combining Data from Multiple Customers** The CPPA seeks comments on the definition of "business purposes" for which service providers and others may "combine" personal information obtained from different sources. Although this issue was addressed in the AG's rulemaking process, the invitation for comment raises the question on whether the CPPA may further limit a service provider's ability to combine personal information. Further restrictions could have a broad impact on everything from security to the development and improvement of artificial intelligence systems.

Aside from these significant topics, the CPPA will also address technical issues that can have a material impact on business compliance processes. These include:

- **Right to Correct:** The CPPA solicits feedback on necessary adjustments to the CCPA rules to incorporate the new consumer right to correct inaccurate personal information.

- **Lookback:** The CPPA requests comment on how to operationalize the twelve-month lookback, focusing in particular on what it means for a company to deny a request for information from beyond twelve months based on the "impossible" or "disproportionate effort" standards described in the CPRA.

- **Audit Authority:** The CPPA seeks feedback on its authority to audit compliance with CPRA.

- **Definitions:** The CPPA solicits feedback on any necessary changes to CPRA definitions, including the definition of personal information, sensitive personal information, "specific pieces of information obtained from the consumer" (e.g., what must be provided in response to an access request), deidentified, unique identifier, precise geolocation, and dark patterns.

Responses to the CPPA's request for comments are due by November 8, 2021. If you are interested in submitting comments to the CPPA, please reach out to attorneys in the Privacy and Information Security practice group at Kelley Drye for assistance.