wiley

NEWSLETTER

California Set to Begin Potentially Far-Reaching Rulemaking on Privacy

October 2021

Privacy In Focus®

As 2021 draws to a close, businesses subject to California's privacy laws should pay close attention to developments underway in that state that will have broad impacts on compliance strategies. On September 22, 2021, the California Privacy Protection Agency (CPPA or Agency) – the new agency established by the California Privacy Rights and Enforcement Act (CPRA) – released an Invitation for Preliminary Comments on Proposed Rulemaking (Pre-Rulemaking Invitation for Comments). This action is the first step in a rulemaking process that will have significant impacts on companies' compliance obligations. Further, two weeks later on October 4, 2021, the CPPA selected Ashkan Soltani as the Agency's new Executive Director to carry out the day-to-day operations of the Agency. As Director, Soltani will oversee the CPPA's rulemaking agenda.

These developments mark the beginning of a critical rulemaking process that – together with the CPRA going into effect in 2023 – will reshape the privacy landscape in California, yet again. Businesses that currently are subject to California's current privacy law (the CCPA) should pay close attention, as the new rulemaking process seeks to *both* update existing California privacy regulations *and* adopt new regulations.

Below, we discuss several key issues to be aware of (among many), as well as the timing for what to expect as the rulemaking gets underway. Of note, comments in response to the Pre-Rulemaking Invitation for Comments are due on **November 8**.

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

State Privacy Laws

Key Issues on the Rulemaking Agenda

In the Pre-Rulemaking Invitation for Comments, the CPPA makes clear that stakeholders may comment on "any area on which the Agency has authority to adopt rules." Invitation at 1. However, the Agency has highlighted eight specific topics in which it is particularly interested, including: (1) processing that presents a significant risk to consumers' privacy or security, cybersecurity audits, and risk assessments performed by business; (2) automated decisionmaking; (3) audits performed by the agency; (4) consumers' right to delete, right to correct, and right to know; (5) consumers' right to opt out of the selling or sharing of their personal information and to limit the use and disclosure of their sensitive personal information; (6) consumers' rights to limit the use and disclosure of sensitive personal information; (7) information to be provided in response to a consumer request to know (specific pieces of information); and (8) definitions and categories.

As is evident from the above list, the rulemaking is poised to cover critical issues, and many of them are novel for California's privacy framework. Of particular note:

Cybersecurity audit and risk assessment requirements

The CPRA directed the Agency to issue certain regulations where businesses' processing of personal information "presents significant risk to consumers' privacy or security." § 1798.185(a)(15). These regulations will require such businesses to perform an annual cybersecurity audit and to submit "on a regular basis" a risk assessment for data processing that presents a significant risk. § 1798.185(a)(15)(B).

The Agency's new rules will be significant, as they will define the triggers for and contours of these requirements, which – as set forth in the rulemaking direction to the Agency – are unique from other state approaches in significant ways. For example, the CPRA discusses regular submission of risk assessments to the Agency and annual audits – neither of which are features of the Virginia or Colorado laws. Relevant questions the Agency is asking include:

- When a business's personal information processing presents a "significant risk to consumers' privacy or security." § 1798.185(a)(15).
- What the audit requirement should entail, and what processes are needed to ensure that audits are "thorough and independent." § 1798.185(a)(15)(A).
- What the risk assessment requirement should entail, assessment frequency, and how the risks and benefits of personal information and sensitive personal information should be weighed.

Further, these new rules open the door for *substantive* processing limitations, not simply filing or disclosure requirements. Specifically, the CPRA states, in relation to risk assessments, that there is a "goal of restricting or prohibiting [high-risk] 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." § 1798.185(a)(15)(B). In the Pre-Rulemaking Invitation for Comments, the Agency specifically asks: "when processing that presents a significant risk to consumers' privacy or security should be restricted or prohibited." Invitation at 2.

Automated decisionmaking

Under the CPRA, the CPPA also is tasked with issuing regulations governing access and opt-out rights regarding a business's use of "automated decisionmaking technology," including "profiling." § 1798.185(a)(16). Specifically, the CPRA details that a business's response to access requests must provide consumers with 1) "meaningful information" about how the decisionmaking processes work, and 2) a description of the "likely outcome" of the process to the consumer. *Id.*

The Agency seeks comment on:

- What activities should be considered "automated decisionmaking" and/or "profiling."
- When consumers should be able to access automated decisionmaking information and how businesses should facilitate access.
- What information businesses should be required to disclose.
- The scope of the opt-out right and the logistics of such a right.

This part of the rulemaking may well intersect with work that is being done to develop approaches to artificial intelligence (AI) and use of algorithms, including work at the National Institute of Standards and Technology (NIST) to develop a voluntary AI Risk Management Framework, and this effort in California to regulate certain automated decisionmaking processes should be watched closely.

Consumers' rights to delete, right to correct, and right to know

While the CCPA already gives consumers certain rights (including the right to know and to delete, as well as the right to opt out from sales), the CPRA will add new rights for California consumers, including the right to request correction of inaccurate personal information.

The CPPA seeks comment on regulations facilitating the new right to correct. Specifically, the Agency seeks comment on:

- New rules or rule changes that would help consumers to make requests to correct inaccurate information.
- When and how often consumers should make correction requests.
- How businesses should respond to correction requests, and how to prevent fraud.
- When businesses are exempt from fulfilling the request because it would be "impossible, or involve a disproportionate effort," or because the underlying information is accurate. § 1798.185(a)(9).
- A consumer's right to provide a written addendum to their record with the business, if the business rejects a correction request.

The rulemaking timeline

For stakeholders that want to engage in this preliminary rulemaking activity, the deadline for submitting comments is November 8. The Agency will then start the formal rulemaking process, which will also include opportunities for public comment.

The Agency expects to soon publish a notice of proposed rulemaking, initial statement of reasons (ISOR), and text of proposed regulations over the winter. Additionally, the CPPA anticipates holding public hearings on the proposals, and expects to deliver final regulations to the California Office of Administrative Law (OAL) in mid-May 2022. Final rules must be adopted by **July 1, 2022**.

As the California privacy landscape continues to be a moving target, companies will need to pay close attention to the development of new rules from the CPPA, as they work to come into compliance with the CPRA by January 1, 2023, when the new law goes into effect. These new rules could have effects that reach far beyond current CCPA regulations, to affect use of algorithms, targeted advertising, and internal compliance procedures. Companies should also consider weighing in as draft proposals are released in the coming months.

Wiley's Privacy, Cyber & Data Governance Team has helped entities of all sizes from various sectors proactively address risks and address compliance with new privacy laws, and advocate before government agencies. Please reach out to any of the authors with questions.

Scott Bouboulis, a Law Clerk with Wiley Rein LLP, contributed to this article.