wiley

NEWSLETTER

California Privacy Protection Agency Releases Draft CPRA Regulations

June/July 2022

Privacy In Focus®

On May 27, 2022, the California Privacy Protection Agency (CPPA or Agency) released a much-anticipated draft of the regulations that would implement certain provisions of the California Privacy Rights Act (CPRA). At 66 pages long, these draft regulations cover a wide range of significant topics and issues. However, they do not address all of the rulemaking topics that were laid out in the CPRA, and additional draft regulations are expected to be released.

In this article, we provide a high-level overview of some of the key provisions that these regulations propose, as well as what they leave out. We also provide a forecast of what to expect in terms of next steps as the CPPA moves toward adopting these proposals.

Topics and Issues Covered by the Draft Regulations

The CPPA's draft regulations touch upon key issues in shaping the regulation of privacy practices for businesses, service providers, and contractors under the CPRA. These include:

(1) Restrictions on the Collection and Use of Personal Information (PI)

Generally, the regulations would require that businesses' collection, use, retention, and/or sharing of a consumer's PI be reasonably necessary and proportionate to achieve the purpose(s) for which the PI was collected or processed. To satisfy this "reasonably necessary and proportionate" standard, a business's conduct must be consistent with the expectations of an average consumer. The regulations also provide illustrative examples of how this standard should be applied.

Authors

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Kyle M. Gutierrez
Associate
202.719.3453
kgutierrez@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

State Privacy Laws

(2) Required Disclosures and Communications to Consumers

The regulations require that any disclosures and communications to consumers be easy to read and understandable to consumers, using plain text and straightforward language and avoiding jargon.

(3) Consumer Requests, Consent, and Dark Patterns

Under the regulations, businesses would be required to implement methods for submitting consumer requests under the California Consumer Privacy Act (CCPA) and CPRA and for obtaining consumer consent that incorporate several principles. These principles largely amount to making request and consent methods simple to understand and avoiding consumer manipulation. The principles explicitly apply to language that guilts or shames the consumer for taking a privacy-protective course of action. Of note, the draft regulations state that methods of obtaining consumer consent that do not comply with the draft regulations' principles may be considered dark patterns, and that any agreement obtained through the use of dark patterns does not constitute consumer consent.

(4) Privacy Policies

The regulations would require that privacy policies contain certain elements, including: (1) a comprehensive description of the business's practices for handling PI, including whether the business discloses sensitive PI for purposes other than those authorized by the CPRA and the draft regulations; (2) an explanation of a consumer's rights under the CCPA and how to exercise them; and (3) the date the policy was last updated.

(5) Notice at Collection

The draft regulations expand on existing notice at collection requirements by providing that businesses must include a notice at or before the point of collection of the categories of sensitive PI that are collected, whether PI is sold or shared, how long the business intends to retain PI, and the names of third parties (as opposed to the categories of third parties) that the business allows to control the collection of PI (if any). Further, under the proposed rules, in the case of a business that allows a third party to collect PI on the business's behalf, both the business and the third party would need to provide a notice at collection – which in many cases could lead to consumers receiving multiple notices in the same user experience.

(6) Sensitive PI

The CPRA requires that a business that processes sensitive data must provide the consumer with notice and permit the consumer to use a "Limit the Use of My Sensitive Personal Information" link to constrain certain data processing, which can be referred to as the right to limit. Under the draft regulations, this notice must describe the consumer's right to limit and instruct consumers on how to submit a limitation request, and the link to effectuate this right must be conspicuous.

The regulations also carve out seven purposes for which a business may use or disclose sensitive PI without having to offer consumers the right to limit. These include using or disclosing data in a way reasonably expected by the average consumer in the course of providing goods or services to that consumer, to detect

data security incidents, and to ensure the physical safety of natural persons.

(7) Consumer Links

The draft regulations require consumers be provided links through which they can effectuate their rights, including: (1) links to opt out of selling or sharing PI; (2) links to limit the use of sensitive PI; and (3) an optional alternative opt-out link where consumers can simultaneously opt out of selling or sharing their PI and limit the use of their sensitive PI. These links must generally be conspicuous and either immediately effectuate the consumer's request or direct the consumer to a page where they can learn more about the request they are trying to effectuate before making that choice.

(8) Responding to Consumer Requests

The regulations detail how businesses must handle consumer requests to effectuate their rights, which include: (1) requests to delete; (2) requests to correct (which is a new consumer right under the CPRA); (3) requests to know; (4) requests to opt out of the sale or sharing of PI, including processing opt-out preference signals; (5) requests to opt in after opting out of the sale or sharing of PI; and (6) requests to limit the use and disclosure of sensitive PI.

The business's specific obligations depend on the request in question. Of note, with regard to handling opt-out requests, the draft regulations include a *requirement* that businesses process opt-out preference signals, which is in tension with the language in the CPRA that specifies that doing so is optional. Additionally, the regulations indicate that cookie management tools are not necessarily sufficient to comply with requests to opt out of the sharing or selling of PI or requests to limit the use of sensitive PI.

(9) Data Processing Contracts

The draft regulations lay out several required elements for data processing contracts between businesses and service providers and contractors. These include prohibiting the service provider or contractor from selling or sharing PI, identifying the specific business purposes for which PI is to be processed, and prohibiting the service provider or contractor from using or disclosing the PI for any other purpose. As for contracts with third parties, an identification of the purpose for which the PI has been sold or disclosed must be included, among other requirements.

(10) CPPA Enforcement and Audits

The draft regulations lay out the process by which a sworn complaint can be filed with the CPPA alleging a violation. Under the regulations, the CPPA has fairly broad discretion to initiate investigations. Once it does, it must hold a proceeding to determine probable cause, issue a notice of probable cause, and hold a hearing on the matter.

Additionally, the draft regulations would allow the Agency to perform audits to ensure compliance. Under the proposed regulations, the CPPA would be able to conduct audits (1) to investigate possible violations of the CCPA; (2) if the audit subject's collection or processing of PI presents significant risk to consumer privacy or

security; or (3) if the audit subject has a history of noncompliance with the CCPA or other privacy law.

Topics and Issues *Not* Covered by the Draft Regulations

There are additional topics that the statute requires the CPPA to promulgate rules about that are not included in these draft regulations. For example, the regulations do not address:

(1) Requirements for certain businesses to annually perform cybersecurity audits and regularly submit risk assessments to the CPPA.

(2) Rules for opting out of automated decision-making technology.

(3) Technical specifications for opt-out preference signals.

Relatedly, the requirements in the draft regulations for data processing agreements do not match the requirements in the CPRA, and in some cases appear to go beyond the statutory requirements.

Next Steps

In addition to the draft regulations themselves, the CPPA also released an initial statement of reasons detailing the Agency's authority to issue the regulations and explaining the purpose and necessity behind the proposals. Further, in a meeting on June 8, 2022, the CPPA voted to formally kick off the rulemaking process under the CPRA. An official comment deadline has not yet been announced, but once the comment period opens stakeholders will have 45 days to submit written comments to the Agency, meaning that the CPPA will miss its July 1, 2022 statutory deadline to adopt the CPRA regulations. The Agency will also be holding a public hearing as part of the rulemaking process.

Looking ahead, it is important to remember that these regulations are merely in draft form and will likely be modified during the rulemaking process. While exact timing for when the final rules will be adopted is still uncertain, entities that do business in California will surely want to monitor the comments that the CPPA receives to see how the final iteration of these regulations could be influenced.

Finally, it is also important to view these draft regulations as part of broader shifts in the privacy landscape. Other states will also be enacting omnibus privacy laws in 2023, and notably, Colorado is engaging in a parallel rulemaking process under its new omnibus privacy law. Companies will need to assess the operational compatibility between the proposed rules in California with other developing state frameworks. At the same time, at the federal level, several key leaders in Congress recently released the draft federal American Data Privacy and Protection Act, which would (as currently drafted) for the most part preempt state privacy laws and regulations like these draft regulations.

***

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 regulations. Please reach out to any of the authors with questions.