



COMMENTARY  
JULY 2022



## With New Proposed Regulations, the California Privacy Protection Agency Begins its Rulemaking

### IN SHORT

**The Situation:** The California Privacy Protection Agency ("CPPA") Board has initiated the formal rulemaking process for the first time, implementing many key California Privacy Rights Act ("CPRA") provisions.

**The Issues:** The proposed regulations are extensive and, if implemented in their present form, will require companies to operationalize many new rights and concepts under the CPRA. The proposed regulations are subject to change after the initial public comment period.

**Looking Ahead:** Businesses should start reviewing and developing their privacy compliance processes now to be ready to comply when the CPRA goes into effect in January 2023.

On July 8, the CPPA [officially began](#) the formal rulemaking process for new privacy regulations—many of which operationalize new CPRA requirements. With the [publication](#) of the Notice of Proposed Rulemaking, the 45-day initial public comment period has begun.

The proposed regulations are divided into nine substantive articles and address a variety of topics, including consent, required privacy notices and disclosure to consumers, mandatory user opt-out signals, and provisions related to sensitive personal information. The regulations are partial: they do not address all areas for which the CPRA contemplates regulations. Additional regulations with respect to these other areas, including privacy risk assessments and cybersecurity audits, are expected later. This Commentary highlights key provisions of the proposed regulations under the CPRA applicable to entities doing business in California.

### **Update Privacy Policy and Internal Processes to Allow Consumers to Exercise New CPRA Rights**

A major compliance area for businesses is operationalizing new CPRA rights—specifically, the right to correct inaccurate personal information and the right to limit use and disclosure of sensitive personal information. Businesses will need to consider reviewing and updating their privacy policies and processes to account for these new rights and to allow consumers to exercise them in a timely manner as prescribed in the statute.

These compliance obligations are significant. For the right to correct inaccurate personal information, businesses not only need to correct the information in their existing systems, but also must take steps to avoid re-introducing the inaccuracy later and must obligate their service providers to correct the inaccurate information. For the right to limit use and disclosure of "sensitive personal information"—a new concept under CPRA—businesses need to provide two or more methods for consumers to exercise this right. In deciding which methods to provide, a business must consider how it interacts with consumers and how it collects sensitive personal information, among other factors.

### **Avoid Dark Patterns that Confuse or Impair Consumer Decision-Making**

The proposed regulations provide considerable guidance on how businesses should obtain consent from consumers and the methods they use to let consumers exercise their privacy rights. As

proposed, the regulations prohibit the use of dark patterns—defined as a user interface element that "has the effect of substantially subverting or impairing user autonomy, decision-making, or choice, regardless of a business's intent."

Avoiding dark patterns requires businesses to, in general, not use language or processes that confuse and manipulate consumers or impair their decision-making and, importantly, provide "symmetry in choice" when consumers exercise their privacy rights. "Symmetry in choice" means that the process for a consumer to make a more privacy-protective choice cannot be longer or substantively different than when making a less privacy-protective choice. For example, if a website banner allows a consumer to opt-out of the sale of personal information, a symmetrical choice would be two options that "Allow Sale" or "Decline Sale." It would not be a symmetrical choice if the two options were "Allow Sale" or "Preferences" because it would require the consumer to take additional steps to "Decline Sale" by first navigating to "Preferences."

### Respect the Opt-Out Preference Signal

The proposed regulations embrace a mandatory opt-out signal that consumers can use to opt out of the sale or sharing of their personal information. If a consumer has an opt-out preference signal enabled—for example, an HTTP header—businesses will be required to treat the signal as a valid consumer request to opt-out of the sale or sharing of their personal information. But if the opt-out signal conflicts with a previous consumer consent or setting that allowed the business to sell or share the consumer's personal information, businesses are allowed to notify the consumer about the conflict and ask to re-consent.

The prevailing understanding of CPRA requirements until now was that businesses could either provide a link to opt out or honor the opt-out preference signal to enable consumers to tell the business that they do not want their personal information sold or shared. However, the draft Initial Statement of Reasons ("[ISOR](#)") accompanying the proposed regulations specifically note that this clarity was provided "to respond to incorrect interpretations in the marketplace that complying with an opt-out preference is optional for the business."

### Next Steps

The 45-day initial public comment period will end on Aug. 23, 2022, at 5 p.m. If the CPPA proposes any substantive changes to the proposed regulations after the initial comment period, it will open an additional public comment period for at least 15 days and consider any comments received on those proposed modifications.

## THREE KEY TAKEAWAYS

1. The requirements under the CPRA and its proposed regulations are extensive. The proposed regulations are likely to undergo modifications during the public comment period. However, it is unclear whether they will be finalized before the CPRA comes into effect on January 1, 2023, adding increased uncertainty to businesses reviewing privacy programs for compliance.
2. Businesses should anticipate another round of regulations on other key CPRA provisions, including privacy risk assessments, cybersecurity audits, and automated decision-making.
3. Businesses should begin reviewing their practices now to identify compliance gaps with new requirements introduced by the CPRA, including assessing whether they collect sensitive personal information and assessing whether consent procedures could meet the definition of dark patterns.



Lisa M. Ropple  
Boston



Jennifer C. Everett  
Washington



Mary Alexander Myers  
Atlanta




Mauricio F. Paez  
New York



Jeff Rabkin  
San Francisco / Silicon Valley



Kerianne N. Tobitsch  
New York



*Amul Kalia, an associate in the San Francisco Office, contributed to this Commentary.*

Jones Day is a global law firm with more than 2,400 lawyers on five continents. One Firm Worldwide®

**Disclaimer:** Jones Day's publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information purposes only and may not be quoted or referred to in any other publication or proceeding without the prior written consent of the Firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our "Contact Us" form, which can be found on our website at [www.jonesday.com](http://www.jonesday.com). The mailing of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the authors and do not necessarily reflect those of the Firm.

© 2022 Jones Day  
North Point, 901 Lakeside Avenue, Cleveland, Ohio 44114-1190  
[www.jonesday.com](http://www.jonesday.com)