

Calif. Privacy Agency Officially Starts Clock On Rulemaking

By **Allison Grande**

Law360 (July 11, 2022, 9:12 PM EDT) -- California's new privacy agency has set an Aug. 23 deadline for stakeholders to weigh in on its first effort to craft regulations to guide companies in implementing tighter restrictions on how they use and share consumers' personal information, marking the first step in its highly anticipated rulemaking process.

While the California Privacy Protection Agency quietly released the first draft of its regulations at the end of May, the agency took the long-awaited step of beginning the formal rulemaking process Friday, when it issued a Notice of Proposed Regulatory Action to draft and adopt rules for the California Privacy Rights Act, a strengthened version of the state's landmark Consumer Privacy Act that is set to take effect in January.

Businesses, consumer advocacy groups, academics and others who wish to offer their feedback on the proposed regulations have until Aug. 23 to submit written comments, and the agency plans to gather additional input at public hearings Aug. 24 and 25, according to Friday's announcement.

"The Notice of Proposed Rulemaking is significant because it kicks off the formal comment period for the draft CPRA regulations, which will conclude with [the] public hearings," Reece Hirsch, co-head of the privacy and cybersecurity practice at Morgan Lewis & Bockius LLP, told Law360. "Because the draft regulations contain many significant departures from the text of the CPRA statute, comments should be extensive, and the August hearings should be lively."

The proposed regulations put forth by the agency Friday do not appear to differ materially from the draft rules released in May, Hirsch said.

Like the draft regulations, the proposed rules offer insights into how companies' obligations to provide consumers with the ability to access, delete, correct, and stop the sale or sharing of their personal information under the Consumer Privacy Act currently in effect will change under the CPRA.

The proposed regulations touch on several vital topics for businesses, including privacy notice requirements, the obligation of companies to notify their service providers or contractors to delete personal information and how to respond to opt-out preference signals.

Companies must treat these browser signals, which users can "easily" engage to exercise their right to opt out of the sale or sharing of their data "with all businesses they interact with online without having to make individualized requests with each business," as a valid request to cease these practices, the

proposed regulations state.

The agency also proposes placing enhanced obligations on third parties that handle consumer data, including by requiring both businesses and the service providers they contract with to provide notice to consumers at the time of collection about what data is being gathered and how it's being used and shared and to honor consumer requests to delete or opt out of the sale or sharing of data.

Other notable provisions in the proposed regulations include that businesses must by default provide consumers that lodge access requests with all of their personal information dating back to Jan. 1, 2022, rather than just from the previous 12 months; that companies that process information for a reason "incompatible" with the purpose for which it was originally collected obtain fresh consent; and that failure to follow the rules for obtaining consent and allowing consumers to submit requests shall be deemed a "dark pattern."

Following the release of the draft regulations, compliance attorneys and consumer advocates predicted that the California privacy agency would receive a crush of feedback on its proposal, which tackles rulemaking topics like browser privacy signals and dark patterns that other regulators have yet to touch and has stoked concerns about a lack of harmonization between the California rules and other state privacy law regimes.

The California privacy agency has attempted to allay these concerns by insisting that its proposed rules "take into consideration privacy laws in other jurisdictions" and that following them "would not contravene a business's compliance with other privacy laws," including state statutes and the European Union's General Data Protection Regulation.

Some experts have argued, however, that the draft regulations would establish a highly technical regime that, if it stands, would be difficult to reconcile with the other laws in this area.

During the public comment process, trade groups are expected to focus on the workability of the technical requirements of the proposed regulations, including the difficulties that they would argue businesses will have with honoring global privacy signals that are not clearly defined, while advocacy groups will push for the agency to continue to put pressure on companies and resist efforts to weaken the regulations, experts have said.

While the July 1 deadline that the CPRA had set for the privacy agency to finalize regulations has passed, "it seems that the agency is now seeking to move relatively quickly to finalize the CPRA regulations, which will be necessary in order to give businesses time to prepare for the Jan. 1, 2023, compliance date," Hirsch, the Morgan Lewis attorney, said.

Companies should also be on the lookout for agency guidance on the aspects of the CPRA that are not addressed in the proposed regulations but that the regulator will need to address before the end of the rulemaking process, including exemptions for employee and business-to-business data, cybersecurity audits and privacy risk assessments, according to Hirsch.

"Businesses should begin developing the broad strokes of a compliance program to meet the new requirements of the CPRA, even though the regulations are a work in progress," Hirsch said.

--Editing by Peter Rozovsky. All Content © 2003-2022, Portfolio Media, Inc.