LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Calif. Privacy Agency Signals Strength With Rules Proposal

By **Allison Grande**

Law360 (June 17, 2022, 5:05 PM EDT) -- California's new consumer privacy agency proposed strict guardrails in its first foray into rulemaking for topics such as global opt-out signals and dark patterns that other regulators have yet to touch, with reactions from digital advertisers and other businesses expected to follow.

The California Privacy Protection Agency, the only dedicated privacy regulator in the U.S., late last month quietly released the first draft of its highly anticipated regulations for the California Privacy Rights Act, a strengthened version of the state's landmark Consumer Privacy Act that's set to take effect in January.

The draft touches on several key topics for businesses, including privacy notice requirements, the obligation of companies to notify service providers or contractors to delete personal information, and how to respond to opt-out preference signals. It elaborates upon and extends the mandates found in the CPRA, "creating what is likely to be, by far, the most prescriptive and consumer-oriented privacy framework in the U.S.," said Reece Hirsch, co-head of the privacy and cybersecurity practice at Morgan Lewis & Bockius LLP.

"The agency has certainly announced its intent with these draft regulations to create a uniquely detailed and consumer-focused privacy regulatory regime in California and, by extension, throughout the U.S.," Hirsch said.

Virginia, Colorado, Utah and Connecticut have followed California in putting comprehensive consumer privacy legislation on the books, but only the Golden State has a dedicated agency to implement and enforce the law. It is also the only state to delve with such granularity into issues such as browser privacy signals, dark patterns and third-party contracting requirements, said Kirk Nahra, co-chair of the cybersecurity and privacy practice at WilmerHale.

"California has taken the lead on these topics by being the first to provide explicit requirements on these issues," Nahra said.

Although other states and regulators may follow California's example, attorneys who advise companies on compliance say they are troubled by a lack of harmonization in the draft with the growing patchwork of state privacy laws.

"It's becoming pretty clear that California may be on the leading edge, but it's kind of out of step with

what other states are doing," said Robert Braun, co-chair of the cybersecurity and privacy group at Jeffer Mangels Butler & Mitchell LLP.

The agency pushed back on this concern a week after the draft regulations were published with an "initial statement of reasons."

In that document, the CPPA asserted that its latest 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.

"In doing so, [the draft regulation] simplifies compliance for businesses operating across jurisdictions and avoids unnecessary confusion for consumers who may not understand which laws apply to them," the agency said.

Several compliance attorneys disagreed, arguing that the draft regulations establish a regime that, if it stands, would be difficult to reconcile with the other laws in this space.

"The regulations, as written, impose highly technical contractual and disclosure obligations that differ fundamentally from other privacy laws and will confuse businesses and consumers," said Daniel Goldberg, chair of the privacy and data security group at Frankfurt Kurnit Klein & Selz PC. "I hope the CPPA will reduce many of these technical requirements in the next round."

With the proposed regulations finally revealed, attention now turns to how the agency will react to the anticipated flood of public comments once the draft is published in the California Regulatory Notice Register. Businesses and privacy advocates are expected to be heavily involved in this process once it's officially opened.

Trade groups will likely focus on the workability of the technical requirements of the proposed regulations, including the difficulties that they'll argue businesses will have with honoring global privacy signals that aren't clearly defined, while advocacy groups will push for the agency to continue to put pressure on companies and resist efforts to weaken the regulations.

"They've divided down those lines before," including when submitting feedback to California's attorney general on proposed CCPA regulations, "and I wouldn't be surprised if that continued," said Braun of Jeffer Mangels.

Alan Butler, executive director and president of the Electronic Privacy Information Center, called the draft regulations "an important first step" in achieving a stronger level of data protection for consumers.

"The agency really has to flex its significant muscles under this regulation to show that it's not going to cave to pressure from industry to whittle away at the protections included in the statute and regulations," Butler told Law360.

Butler praised the agency for clearly stating that companies must treat all signals that consumers can use to opt out of the sale or sharing of their data across all websites as a valid request to stop these practices, without having to make individualized requests with each business. In doing so, the agency rejected some industry members' stance that businesses should have a choice between posting a do-not-sell-or-share link or honoring an opt-out preference signal.

"They're arguing that the statute doesn't do what it's clearly intended to do, which is make it simple and seamless for users to set a global privacy setting in one click instead of having to tell a whole bunch of different entities separately to not sell or share their data," Butler said. "So it's good to see the agency push back on that."

While the agency still needs to issue regulations on more than half of the 22 regulatory topics under its rulemaking authority, including cybersecurity audits and privacy risk assessments, "there's nothing troubling us yet," Butler said.

"They've begun to tackle some important issues, such as mandating global opt-outs and addressing dark patterns, and that shows that the CPPA is ready to put forward strong regulations and be aggressive in enforcing consumer privacy rights," Butler said.

On the business side, digital advertisers are likely to comment on how the draft regulations' limitations on the sharing and selling of data are likely to affect their operations, according to compliance attorneys.

"The biggest impact here is on the digital advertising industry," said Alysa Z. Hutnik, chair of the privacy and information security practice at Kelley Drye & Warren LLP. "There are multiple ways throughout the 66 pages of the draft regulation that digital advertising and analytics are reclassified and restricted in ways that depart from both the text of the CPRA and other state laws."

The proposed regulation's mandate that businesses have a process for responding to global opt-out digital signals is likely to be a main point of contention throughout the process.

"As it's currently drafted, the requirement is way too broad, and there are not enough qualifiers or explanations about what signals need to be recognized," said Goldberg of Frankfurt Kurnit.

Given that there's a growing array of tools being made available for consumers to signal their opt-out preference, expressly naming a universal recognized mechanism like the Global Privacy Control would be helpful, attorneys say. But the proposed regulations decline to take such a step, instead embracing a broad definition that is likely to encompass a range of privacy signals, including some that companies many not have the technical capabilities to look for or identify.

"They're assuming that someone is going to step into the breach and develop a technical answer for honoring these signals that doesn't yet exist," Braun said. "If there were a more consistent and universal approach [to honoring consumer opt-outs], then it might be easier to do. But right now, it's just a mess."

The proposed regulation, if finalized, could also "cause businesses to engage in significant work to update contracts" due to the enhanced notice and compliance obligations they place on data controllers and their third-party service providers, said Hirsch of Morgan Lewis.

This includes the mandate for businesses that disclose personal information to another company for purposes such as targeted advertising to enter into an agreement with the third party that identifies in non-generic terms the "limited and specified purpose(s) for which the personal information is sold or disclosed."

Both parties would also be required 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.

"The purpose of privacy laws like CPRA is to provide individuals with more information about and choice around how their information is being used," Goldberg said. "Where things go wrong is when there are a lot of technicalities and granularities that require businesses to make even more disclosures that may not necessarily help consumers."

While there's much to unpack in the CPPA's first rulemaking offering, attorneys stressed that there's still a long way to go.

"The first thing for companies to do is take a deep breath," said Kelley Drye's Hutnik. "These draft regulations are ambitious, and what we've learned in all prior rulemakings is that things get updated in response to comments, particularly ones that raise issues that the agency hadn't meaningfully considered yet."

The agency also still needs to issue a second round of draft regulations to address other areas under the agency's authority, such as the status of the exceptions relating to employee and business-to-business data, privacy risk assessments and cybersecurity audits, according to Hirsch.

"The CPRA requires the CPPA to finalize regulations by July 1, but given the complexity of this draft and the topics that remain to be addressed, it's hard to imagine the regulations being finalized by [the law's] Jan. 1, 2023, effective date," Hirsch said. "That means that businesses would be well-served to begin making high-level plans for CPRA compliance."

In working to comply with the law before the regulations are finalized, companies should "take a step back and look at the bigger picture" of what's required by the CPRA, according to Braun.

That will allow companies to separate the more thorny and evolving compliance issues, such as how to interpret opt-out signals and what needs to be in contracts with third parties, from the more solid provisions that can be put in place now, such as the requirement to implement a system for allowing consumers to exercise their rights to access, delete and correct their personal information, attorneys say.

"Companies should go through the CPRA and identify those consumer protection rights outside of advertising that look like they're only going to change around the edges," Hutnik said. "That will allow companies to focus on putting the scaffolding up around those areas, while pushing further down the calendar areas closer to the advertising industry that may change more significantly."

--Editing by Brian Baresch and Kelly Duncan.
