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 Enforcement To Heat Up As Regulation Matures

By **Allison Grande**

Law360 (September 3, 2021, 5:56 PM EDT) -- The California attorney general's willingness to work with companies to comply with the state's novel consumer privacy law was on full display in its first year of enforcement, but pressure is expected to ramp up as businesses lose their ability to cure deficiencies and consumers are given more power to flag violations.

The AG's office in July pulled back the curtain on its enforcement activities under the California Consumer Privacy Act. Since it began policing the law on July 1, 2020, the office revealed, it has issued dozens of notices of noncompliance to online retailers, media outlets, marketing companies, data brokers and other businesses suspected of failing to meet their new obligations to ensure that consumers are able to access, delete and opt out of the sale of their personal information.

"It's become clear that the attorney general's office is very focused and serious about enforcing the law, so the takeaway for companies should be that if they haven't taken CCPA compliance seriously or have put in minimal effort, they need to do another review of the CCPA and update their policies," said Jacqueline Cooney, lead director of the data privacy and cybersecurity practice group at Paul Hastings LLP.

Attorney General Rob Bonta's latest announcement also highlights the importance of being able to react quickly if a problem is identified. According to the attorney general, 75% of businesses that received a notice from his office acted to come into compliance within the 30-day period that the law allows for companies to cure alleged missteps, while the remaining 25% of businesses that received these notices were either still under the 30-day cure period or faced pending investigations.

"What's been particularly noteworthy is how the curative provision has worked as a tool to promote compliance with the law during the first year of enforcement," said Mark Krotoski, co-head of the privacy and cybersecurity practice at Morgan Lewis & Bockius LLP, adding that most laws don't afford companies such an opportunity to fix issues before a regulatory probe is opened.

Businesses, however, won't be able to rely on this provision much longer. The California Privacy Rights Act, which is set to replace the CCPA at the beginning of 2023, removes the cure provision, meaning that both the state attorney general and the new California Privacy Protection Agency tasked with policing data privacy violations will be able to initiate enforcement proceedings without having to provide companies with a chance to correct deficiencies.

"That's significant because it seems like most companies are using the cure period to go back and make

changes, so without the cure period, they may be in trouble," said Cynthia Cole, a partner and deputy department chair of the corporate section at Baker Botts LLP.

The attorney general's already active monitoring of companies is only expected to increase in the coming months, especially in light of Bonta's July announcement of the rollout of a new online tool that allows consumers to notify businesses of potential violations directly.

The Consumer Privacy Tool is designed to ask "guided questions to walk consumers through the basic elements of the CCPA" before generating a notification that users can then email to businesses that they believe don't have a clear and easy-to-find "Do Not Sell My Personal Information" link on their websites or mobile apps. This email "may trigger the 30-day period for the business to cure their violation of the law," according to Bonta, who additionally encouraged consumers to actively exercise their new CCPA privacy rights.

"The attorney general's statement that consumers can and should join enforcement efforts shows that it won't just be his office policing the law, but California residents as well," said Shannon Yavorsky, a partner in the cyber and privacy practice at Orrick Herrington & Sutcliffe LLP.

Bonta, a Democrat and former member of the California State Assembly, took over the reins at the attorney general's office in April.

"The new attorney general's focus really seems to be on making it easy for consumers to not only exercise their rights, but also to complain and make their voices heard," Cooney said, noting that the CCPA only allows consumers to bring private lawsuits for companies' data security failings and not if their new privacy rights haven't been honored.

"This new tool gives consumers an avenue for making sure that they're helping to hold companies accountable," Cooney added, "and in some ways it does put some extra urgency on companies to comply, since now anybody can lodge a complaint, and it's another way for the attorney general to be alerted if a company isn't being compliant."

As enforcement intensifies, companies should look at the 27 generalized resolved case summaries that the attorney general published in July for insights into the regulator's expectations and how to comply with the novel law, attorneys say.

"If a company is concerned about what the attorney general is focusing on, these summaries are a really good tutorial about what companies have been dinged for," Cooney said.

The attorney general characterized the summaries, in which general descriptors were used in the place of company names, as "illustrative examples of situations in which it sent a notice of alleged noncompliance and steps taken by each company in response," while stressing that the disclosures didn't constitute legal advice.

The examples included a car business updating its privacy policy after it allegedly failed to inform test drivers of the use of their personal information at the point of collection; a grocery chain amending its privacy policy to provide a notice of financial incentive to shoppers who provided personal information in exchange for participation in its loyalty programs; a social media app submitting detailed plans about its consumer response procedures to cure concerns that it was not timely responding to these requests; and an online dating platform adding a "clear and conspicuous 'Do Not Sell My Personal Information'""

link to its homepage after being alerted by the attorney general of potential noncompliance.

David Manek, senior managing director of cybersecurity and data privacy at Ankura Consulting Group LLC, noted that when the attorney general's office began issuing letters of noncompliance, the alleged violations "were mostly surface level in nature."

"For example, perhaps the OAG cited the organization's failure to include instructions on how an authorized agent should submit a request on behalf of a consumer, or perhaps the organization didn't specifically make reference that they had no knowledge of a sale of minors' data," Manek said. "These surface-level items were easy to fix in the cure period."

More recent waves of letters have been focused on "proving out statements" made in these notices, such as confirming that a company has the appropriate contracts in place to limit the processing of data transferred to third parities, according to Manek.

The 27 examples of CCPA noncompliance laid out by the attorney general make clear that the office is "focused on two main themes": that organizations are providing clear instructions and processes to support the consumer rights response process and that businesses are adequately operationalizing their obligations to ensure consumers are able to stop the sale of their data, Manek said.

During the past year, the attorney general's office has "focused substantially" on the CCPA's do-not-sell right, noted Kyle Fath, of counsel at Squire Patton Boggs.

This attention has come as little surprise, given the widespread uncertainty that has swirled since the law took effect in January 2020 over whether the sharing of personal information for targeted advertising purposes constitutes a "sale" covered by the CCPA.

While the attorney general has not publicly opined whether a "sale" occurs when a third-party cookie provider collects information on a website, the case summaries provided by the regulator indicate that its apparent position is that a "sale" happens when a website owner makes personal information available to third-party cookie providers with which it hasn't established a service provider relationship, according to Fath.

"In view of this new clarity on the 'sale' issue, most organizations will need to revisit their current approach to the 'Do Not Sell' obligation with respect to digital advertising," Fath said.

Given the attorney general's recent launch of the tool that allows consumers to lodge complaints with companies that don't prominently display a way to opt out of data sales, and his push for companies to honor a mechanism known as the Global Privacy Control for consumers to broadly signal to the websites they visit that they want to stop these sales, "it appears likely that there will continue to be a focus on the Do Not Sell issue with AG Bonta," Fath added.

The CPRA, which takes effect Jan. 1, 2023, solidifies the sale opt-out, while adding the obligation for companies to enable consumers to also opt out of the sharing of their personal information, including for targeted advertising. This expansion is likely to further enhance the regulator's interest in this topic, while creating additional liability risk for businesses, attorneys say.

"While we don't know what enforcement is going to look like going forward with the CPRA," Cooney said, "we can certainly say that California is going a little deeper into regulating how companies are

processing and sharing personal information, and that's going to continue to be a focus going forward."

--Editing by Orlando Lorenzo.
