LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Unshackled Calif. Privacy Agency To Bring Enforcement Heat

By **Allison Grande**

Law360 (February 16, 2024, 11:14 PM EST) -- California's privacy regulator is expected to not waste any time responding to a recent ruling that cleared the way for the fledgling agency to begin immediately enforcing the rules it's crafted under the state's data protection law, making it vital for businesses and employers to adjust their compliance efforts to meet the accelerated timeline.

While the California Privacy Protection Agency had been poised to begin enforcing a dozen of its new privacy regulations on March 29, which marked a year after the regulator finalized this batch of rules, a California appellate court surprised many when, after months of having the dispute before it, the three-judge panel unanimously ruled on Feb. 9 that there was no reason for the agency to wait until the end of next month to begin its enforcement efforts.

Instead, the appellate court opened the door for the agency to begin enforcement immediately, finding that the trial court was wrong to impose a one-year waiting period for finalized regulations when the California Privacy Rights Act — which voters approved in 2020 to beef up the state's existing consumer data protections — clearly states the nation's first dedicated privacy agency could start flexing its enforcement muscles on July 1, 2023.

"If enterprises have been sitting down on complying, then they will be caught off guard and ill-prepared," said Cynthia Cole, a data privacy partner at Baker McKenzie. "The CPPA has had a lot of time, as well, to think about their enforcement strategy and prepare for it, so I think we should expect to see action quickly."

The CPPA has left no doubt of its short-term plans, with the agency's Deputy Director of Enforcement Michael Macko saying in response to the appellate court's ruling that its enforcement team "stands ready to take it from here" and warning companies that the decision should "serve as an important reminder" that "now would be a good time to review your privacy practices to ensure full compliance with all of our regulations."

These comments echoed those made by several California enforcement officials at a privacy summit held by the California Lawyers Association on Feb. 8 and 9, a gathering that sent the clear message that "we all better buckle up," noted Kyle Fath, a summit attendee and Los Angeles-based partner in the data privacy, cybersecurity and digital assets practice at Squire Patton Boggs LLP.

During the summit, Macko spoke in depth about the agency's power to issue both administrative cease-and-desist orders and administrative fines, according to Fath.

The deputy enforcement director noted that both remedies have the potential to have a significant impact on companies, given that the agency can issue fines of up to $7,500 for each of the "hundreds or even thousands of violations" it's typically looking at in each investigation, and its administrative relief powers include nonmonetary orders such as halting certain activities that "could threaten a company's existence," Fath added.

However, despite the recent rhetoric from the agency's leadership, robust enforcement right out of the box isn't necessarily a given.

While the agency has announced it's looking into the data privacy practices of connected car manufacturers, the nascent regulator has to date been primarily focused on writing regulations and has yet to publicly engage in any "substantial enforcement activity," leaving questions about if and when these efforts may pick up, noted Kirk Nahra, co-chair of the cybersecurity and privacy practice at WilmerHale.

"I would mainly expect that this earlier effective date presents an opportunity to start gathering information and potentially starting investigations down the road," Nahra said. "It just makes the runway that they will give companies to get up to speed start a little earlier."

Under the California Privacy Rights Act, which builds on the state's first-in-the-nation privacy law and cements rights for consumers to access, delete, correct and stop the sale and sharing of their personal information, the CPPA was charged with establishing regulations for 15 different topics. The law and regulations also apply to data collected in employment and business-to-business contexts, with California being the only state so far to not exempt these categories from its comprehensive privacy law.

While the statute required the CPPA to finalize its regulations by July 1, 2022, the agency didn't complete its first batch of regulations until March 29, 2023. This set addressed a dozen of the areas the agency was given to tackle, including privacy notice requirements and how to respond to browser signals that communicate consumers' choice to opt out of the sharing of their personal data.

The day after these regulations were finalized, the California Chamber of Commerce filed a lawsuit challenging the agency's plans to begin enforcing the new rules on July 1, 2023. While this was the enforcement date specified in the statute, the chamber argued California voters had intended for businesses to have a full year to comply with any new rules and that the CPPA's failure to complete its work by the July 2022 deadline meant it couldn't start enforcement until a year after the regulations were put in place, which would be March 29, 2024.

This argument won traction with state court Judge James P. Arguelles, who in a June ruling barred the privacy agency from beginning enforcement until March 29. But in its ruling earlier this month, the state appeals court reversed this finding, concluding that "because there is no 'explicit and forceful language' mandating that the agency is prohibited from enforcing the act until (at least) one year after the agency approves final regulations, the trial court erred in concluding otherwise."

The ruling is poised to impact not only the finalized slate of regulations but also future regulatory efforts, including the agency's highly anticipated upcoming launch of formal rulemaking for the remaining three topics of risk assessments, cybersecurity audits and regulating technologies fueled by artificial intelligence, attorneys noted.

"Covered entities should be prepared for immediate enforcement of future regulations, which may be

enforced upon finalization," Cole of Baker McKenzie noted. "This will give businesses a potentially very small window to prepare."

For the regulations that were finalized last March, companies have had more lead-in time, which is likely to somewhat blunt the impact of the court's ruling, which was handed down less than two months before the original March enforcement deadline.

"Fortunately, businesses have had the regulations in hand for almost a year, and in my experience most have already prepared," noted Kristen Mathews, a partner at Morrison Foerster LLP.

Usama Kahf, co-chair of Fisher Phillips' data security and workplace privacy practice group, agreed that the appeals court's ruling was more of a "wake-up call" for companies and employers, especially given that only the agency's ability to enforce the rules had been enjoined until next month.

"There are some companies that have wrongfully and incorrectly assumed that March 29, 2024, was their compliance deadline," Kahf noted. "But the regulations took effect last March, and the agency can still look back at that time period when it begins enforcement."

In its enforcement efforts, the agency is likely to look at whether businesses and employers have been engaging in "good faith efforts" to comply rather than "sitting around waiting until the last minute," he said.

"For businesses, what they really need to be doing is to immediately focus on the low-hanging fruit that regulators and the public can see," including privacy policies, vendor agreements and the mechanism that they provide consumers with to opt out of the sale or sharing of their personal information, according to Kahf.

"The agency doesn't have unlimited resources, so it has to be strategic about who it targets," Kahf said, adding that the first enforcement strikes are likely to be instances where the regulator "can identify a common practice or common mistake that a business might make in order to set an example and use it as a way to provide guidance to everyone else."

During the California Lawyers Association's privacy summit earlier this month, the CPPA's deputy enforcement director confirmed that even though the law no longer provides companies with 30 days to cure potential violations, the agency, along with the state's attorney general, "will consider different factors in their investigations," including whether the business "can demonstrate good faith efforts to comply with [the privacy law's] requirements" and whether there are "appropriate equitable remedies available," Squire Patton Boggs' Fath noted.

Additionally, Fath reported that the enforcement chief laid out some of the agency's top priorities, which include whether what businesses are communicating to the public matches what's in their privacy notices, how companies are responding from the legal and technical perspectives to consumer requests to exercise their rights under the law, whether businesses are properly implementing the right to delete, and accessibility for those with disabilities.

This focus on how companies are "operationalizing" their obligations emphasizes that the agency is likely "looking beyond public-facing compliance efforts, such as posted privacy notices, and into how businesses are implementing their [privacy law] compliance program requirements internally, for example, whether businesses are actually processing do not sell request and opt-out consumers out of the sale/share of their

personal information," Fath said.

For businesses that "have largely prepared and merely want to conduct a last-minute check" of their compliance, Morrison Foerster's Mathews recommended several items for these entities to review "now that the CPPA has been let out of the gate."

These steps include ensuring that privacy policy and data collection notices are up-to-date; that businesses that sell personal information or participate in cross-context behavioral advertising have implemented a global privacy control that enables consumers to universally opt out of the sale or sharing of their data across websites in a single step; and that agreements with third parties to which companies sell or share personal information and internal training materials have been updated to cover the additional details outlined in the regulation.

Monique "Nikki" Bhargava, a partner at Reed Smith LLP, agreed that companies should be "double-checking" their compliance with their obligations to honor browser-based signals that consumers set to universally halt the sale and sharing of their data and to ensure that their "privacy policies and notices are reflecting actual practices," stressing that the agency has placed a "huge emphasis" on these areas in recent months.

"The CPPA has made clear not only when this appeals court ruling came out but also when the initial stay was put into place last year that they feel that businesses have had an extended amount of time to come into compliance with the regulations," Bhargava said.

Another notable regulation out of the set the agency finalized last March is the restrictions on deceptive design features known as "dark patterns" that add unnecessary confusion, burden or friction to consumers making a choice, Baker McKenzie's Cole noted.

"If a business is aware of a dark pattern but chooses not to remedy it, the business is liable for a violation of the law, regardless of whether it intended to trick individuals into sharing more personal data," Cole noted.

Additionally, some of the regulatory requirements that can be applied in a straightforward way in the consumer context, including limiting the use and disclosure of sensitive data and giving users the ability to access what data providers hold about them, might not translate as well in the employment and human resources arena, Fisher Phillips' Kahf said.

"Moving forward, someone has got to be the voice for employers to give clarity about how they can comply with rules that are conceived of and written for the consumer context," Kahf said.

The California Privacy Protection Agency is represented by Rob Bonta, Thomas S. Patterson, Paul E. Stein and Natasha A. Saggar Sheth of the California Department of Justice.

The California Chamber of Commerce is represented by Sean P. Welch, Kurt R. Oneto and David J. Lazarus of Nielsen Merksamer Parrinello Gross & Leoni LLP.

The case is California Privacy Protection Agency et al. v. The Superior Court of Sacramento County, case number C099130, in the Court of Appeal of the State of California, Third Appellate District.