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

Do Calif. AG's New Regs Exceed Scope Of Privacy Law?

By **Allison Grande**

Law360 (December 2, 2019, 5:58 PM EST) -- The California attorney general's highly anticipated draft regulations for implementing the state's Consumer Privacy Act may have put the "meat on the bones" of the law, but expanded notice and transparency requirements are likely to generate significant backlash, with business advocates arguing they go beyond what's laid out in the statute.

The California Consumer Privacy Act, which was signed into law in June 2018 and is set to take effect Jan. 1, requires Attorney General Xavier Becerra to develop rules for implementing the first-of-its-kind statute. The law gives consumers the right to find out what data online businesses such as Google and Facebook hold about them, request that the data be deleted and opt out of the sale of the information.

The regulator delivered on this mandate last month by publishing proposed regulations that Becerra said put "the meat on the bones" of the statute.

The regulations offer guidance for several vital aspects of the law, including how companies should go about notifying consumers of their data access rights and handle data requests.

But they also include some unexpected elements that the business community is likely to seize upon during four public hearings to be held across the state this week and in written comments that are due to the regulator's office by Dec. 6.

"What's likely to attract significant attention are areas where the attorney general's office has sort of staked out new territory that's not reflected in the statute," said Reece Hirsch, co-head of the privacy and cybersecurity practice at Morgan Lewis & Bockius LLP.

While the regulations provided "much more detail about how to actually implement the new consumer privacy rights under the CCPA," confusion over how to properly comply with some of the statute's most notable features — including the prohibition on treating consumers differently if they exercise their rights under the law and the requirements for verifying the authenticity of requests — persists, according to Hirsch.

"It's challenging telling companies to prepare to grant consumers these new privacy rights on Jan. 1 when the guidance on how to implement these rights is still a work in progress," he said.

Travis LeBlanc, vice chair of the cyber and data privacy practice at Cooley LLP and one-time senior adviser to former California AG Kamala Harris, said that while the first round of regulations contain shortcomings, the result likely stems from the roughly seven-member privacy unit at the attorney general's office having been handed the almost "Herculean" task of both drafting and enforcing the new complex privacy rules.

With the public comment period winding to a close, attorneys expect plenty of feedback from a wide range of stakeholders about the regulations and are almost certain that the final version of the regulations — expected out in early to mid-2020 — will feature major revisions.

Putting a Price on Consumer Data

One of the biggest outstanding issues regarding the CCPA has been how to interpret the prohibition on treating consumers differently if they exercise their rights to have their data deleted or not shared with third parties. Many businesses had voiced concerns that the restriction would deal a blow to popular services such as loyalty programs that are premised on consumers' exchange of information for benefits.

While the draft regulations do tackle the discrimination issue, the attorney general declined to explicitly declare loyalty programs and similar offerings as being safe from regulatory scrutiny. Instead, the rules say that companies can still offer a different price or service if it is "reasonably related to the value of the consumer's data," and offered several benchmarks that can be used to calculate this value.

Companies are likely to voice their reservations with this setup, given the complexity involved with putting a good-faith estimate on the value of consumers' data and the difficulty with uniformly applying across industries one type of formula.

"The attorney general has attempted to provide a process for justifying those types of financial incentives, but it's likely that most companies will find it to be still fairly confusing and hard to apply in practice," Hirsch said.

These provisions on loyalty programs and incentives may also "lead down the path of treating personal information as a mere commodity, which seems contrary to the original intent of the CCPA," Morrison & Foerster LLP partner Christine Lyon said.

Handling Consumer Requests

Under the draft regulations, companies would be required to go back and obtain a consumer's opt-in consent to use personal information for any purpose that the company hadn't addressed in its original privacy notice, a provision that Lyon said contains "no exceptions, even if the additional use might be compatible with the original purposes disclosed in the notice."

"This opt-in consent requirement would be burdensome for both customers and consumers," Lyon said. "In fact, it would create a consent regime that is even stricter than" the European Union's stringent General Data Protection Regulations.

The attorney general also proposes that businesses should either provide notice directly to consumers before selling data or return to the source and affirm this notice was given when the data was gathered. This mandate could be particularly challenging for data brokers and similar businesses, which don't

directly interact with consumers, noted Phil Recht, managing partner of Mayer Brown LLP's Los Angeles office and co-leader of the firm's public policy, regulatory and political law practice.

"Oftentimes, these businesses get personal information from a source that didn't get the information directly from consumers, and there could be six layers to peel back to find out where this information came from," he said.

Additionally, the regulations specify that companies that receive opt-out requests need to go back to any entity to whom they have sold data in the previous 90 days and instruct them to not resell the data. This requirement is likely to create complications in situations where buyers haven't promised to not resell the data, and therefore can argue they have no obligation to adhere to the seller's after-the-fact request, Recht said.

The requirements around verifying the identity of consumers making data requests presents another area that's likely to attract backlash, attorneys said.

"Many companies were disappointed that the draft regulations didn't provide more or better guidance about how to authenticate a requestor's identity before granting access to a consumer's personal information," Lyon said.

The draft regulations specify that, for the purposes of consumer authentication, companies should match at least three data points provided by the requestor with data points that the company itself holds and has deemed "reliable for the purpose of verifying the consumer."

However, the regulations "give no indication of how to select those 'reliable' data points, or what to do if a company has only data points that would be fairly easy for anyone to find, [such as] name and home address," Lyon said.

Additionally, the regulations require companies to maintain "reasonable security" measures when both verifying and responding to these consumer data requests. But this mandate isn't included in the text of the CCPA, and the regulations don't elaborate on what security standards qualify as reasonable, a point that companies are likely to urge the attorney general to address, Hirsch noted.

Expanding Obligations for Big Data Collectors

One of the more unexpected provisions in the proposed regs centers on the requirement for businesses that annually buy, share, receive or sell the personal information of more than 4 million consumers to compile a number of metrics about the consumer requests it receives and how it responds to them.

These enhanced transparency obligations and the 4-million-consumer threshold are not mentioned in the CCPA, and companies are likely to challenge whether the attorney general's office has exceeded its authority.

"Companies that are subject to this are probably going to have a lot of questions, because the requirements are fairly burdensome and require them to maintain not only standard CCPA policies, but also sort of a report card that has to be made public," Hirsch said, adding that those reports could end up "subjecting those companies to some close scrutiny."

The proposed regulations also appear to draw into their scope service providers that don't have any relationship with companies that qualify as businesses under the law and suggests that businesses need to broadly honor browser plug-ins and other user controls that indicate consumers don't want their information used or shared by the company.

Tackling Overlooked Issues

In drafting the regulations, the attorney general was required to specifically address certain designated issues, including how to provide notice to consumers and how to handle and verify consumer requests.

This mandate meant that other pressing topics that are vital to companies' compliance efforts may not have made the cut and businesses will likely press the attorney general to address these concerns in the next version of the rules, attorneys say.

"There are issues around some of the basic definitions contained in the CCPA that are not clarified in the regulations and about exceptions to the CCPA that would be helpful to get more guidance on, and the regulations also don't address enforcement of the limited private right of action for security breaches," Hirsch noted.

Companies are likely to also push for the next round of regulations to include input on the most recent round of amendments that the California Legislature made to the CCPA, which were signed into law the day after the attorney general issued his regulations.

The revisions included clarification on how employee data fits into the statutory scheme. While employers were given a one-year reprieve from complying with most of the law's obligations, they are still obligated to provide notice of their data collection practices to employees and implement the necessary “reasonable” data security measures required by the law.

“We have a general sense of what notices should look like and are working with a lot of companies to get the notices ready, but it’s still an area where guidance is needed and would certainly be helpful,” Hirsch said.

--Editing by Philip Shea and Kelly Duncan.