THOMSON REUTERS REGULATORY INTELLIGENCE

IMPACT ANALYSIS: CCPA compliance -- Proposed modifications highlight data privacy law's complexity

Published 25 Feb 2020
by Julie DiMauro, Regulatory Intelligence
Expert Analysis

The California Attorney General has proposed changes to the draft regulations implementing the California Consumer Privacy Act, a data-privacy law with implications for national and international firms that have customers in the most populous U.S. state. The proposed changes seek to add clarity and respond to business concerns about the law's breadth and the obligations it imposes on businesses.

The law, known as the CCPA, is the most comprehensive and consumer-focused data privacy law in the United States so far and is a significant regulatory compliance challenge for the businesses subject to it. It went into effect January 1.
The latest proposed changes add clarity to the law's requirements, but experts believe most businesses are feeling overwhelmed and under-prepared to meet the prescriptions under it.

CCPA rights

Under the CCPA, California consumers have the following rights:

- *The right to know*. They must be able to obtain specific information about the collection, use and sharing of their personal information, and the purpose.
- *The right to request deletion.* They have the right to request deletion of their personal information.
- *The right to non-discrimination*. They have the right to not be discriminated against because they exercised their rights under the law.
- *The right to opt out*. They must be able to request that a business not sell their personal information to third parties.

The CCPA applies to any business that: (1) is a for-profit business doing business in California; (2) collects California residents' personal information, and (3) meets at least one of the following thresholds: (a) has more than $25 million in revenue; (b) buys, receives, or shares personal information of 50,000 or more consumers, households, or devices; or (c) derives 50% or more of annual revenue from selling California consumers' personal information.

At the outset, businesses must determine if the law applies to them and, if so, demonstrate a course for achieving compliance, training employees and monitoring business partners.

The proposed modifications

The proposal seeks to clarify the definition of "personal information," saying the term's application depends on whether information can be tied to a particular person or household.

The Attorney General's (AG's) Office says this means that IP addresses that are collected but never linked to specific consumers or households cannot be deemed "personal information."

The proposed modification also to clarify how a business should notify consumers of its information collection policies in a way that is reasonably accessible. The business should post a link on both its introductory webpage, as well as on all webpages where personal details are collected.

The privacy policies of businesses subject to the CCPA must have should identify the categories of personal information disclosed for business purposes or sold to a third party, as well as the categories of third parties receiving that information.

The draft provides an example of what a compliant "Do Not Sell" button, allowing consumers to block sales of their personal information, would look on a business's homepage.

Some pushback – but also acceptance

"The proposed modifications are a little helpful, sure, but we are still wondering on things like what it means to not discriminate against someone who does not give you their data. Businesses are rightfully pointing out that they need to be given data for it to provide a service," said Cynthia Cole, a data privacy expert with law firm Baker Botts in Palo Alto, California.

"Does the law actually target the personal information it collects for another reason -- outside of that central service it is providing -- and if not, shouldn't that be more apparent?" She asked.

Cole says businesses can clearly understand the spirit of the law -- ensuring transparency and the rights to request, delete and opt out of the sale of one's data -- and the evolving guidance coming from the AG's office is helpful, she said.

She advises business to focus on the overall, obvious goals of the law and not get buried in the details. "Ask the AG's office questions now and be able to demonstrate a good-faith effort to comply as soon as possible," she said.

Businesses must recognize that such data privacy rules coincide with consumers' expectations, Cole said. "Most consumers now expect they will have a greater say into how businesses use

their personal data, thanks to high-profile news coverage of consumer data theft and stolen identities," she said.

Consumer awareness has been raised by publicity over technological advances such as facial recognition and location tracking, and by data-privacy initiatives in foreign jurisdictions and other states, Cole said.

The California initiative echoes the EU's General Data Protection Regulation (GDPR), which also has reach outside the bloc. In New York's SHIELD Act, which takes effect in March requires businesses with information about any New York resident to protect it and notify the resident of any security breach.

Microsoft recently announced it will extend CCPA's core rights for people to control their data to all of its customers in the United States.

Kon Leong, CEO at ZL Technologies, a provider of information governance and analytics solutions, agrees that the most recent proposed modifications are helpful and make the law less open to interpretation. And he reminds businesses not to look at the CCPA in a vacuum.

"Businesses are already subject to other laws that place restrictions around the collection and use of consumers' personal data, such as Gramm-Leach-Bliley and the Fair Credit Reporting Act. Businesses should consider how compliance with CCPA obligations tie into those existing obligations," he said.

The law will lead to many class-action lawsuits, Leong said. One class-action suit already has been filed referencing the law, although it does not allege an express violation of the CCPA as a cause of action in the case.

The most significant challenge in meeting the requirements of the law will probably be dealing with silo-ed data that is hard to assemble, he said. Such data that often sits within legacy and unconnected systems. He expects businesses will need better architecture to manage the flow of personal data and governance protocols that go along with the better technology.

Cole and Leong both mentioned the importance of instituting sound practices as soon as possible, to demonstrate a business's good-faith effort to comply.

Those practices include reexamining one's pre-CCPA privacy policy and updating it, plus training all employees on how to handle personal information and consumer requests.

Service-provider agreements must be retooled to include clearly written acceptance of CCPA compliance by each third-party business partner and to spell out which entity handles which aspects of meeting the law's requirements.

Businesses must delegate the role each department and executive plays in helping the business comply, said Melinda Watts-Smith, Senior Vice President of Strategic Relationships at ZL Technologies.

Compliance could include the efforts of chief compliance and risk officers, chief information security officers, general counsel, information technology and human resources professionals, and others.

State rules must be tracked, as more of them weigh in during the period when the United States lacks a coordinated framework for addressing data protection challenges, as it does now, she said.

(*Julie DiMauro, Thomson Reuters Regulatory Intelligence in New York*.)
