Skadden

California Privacy Law: What Companies Should Do to Prepare in 2019

Contributing Partner

Stuart D. Levi / New York

While debates about the need for a federal data protection law continued to heat up in 2018, California enacted its own comprehensive privacy law, the California Consumer Privacy Act (CCPA), creating a de facto national standard for any company that does business involving California residents. The law effectively sets the floor for nationwide privacy protection, since organizations may not want to maintain two privacy frameworks — one for California residents and one for all other citizens.

The CCPA generally gives consumers more information and control over how their data is being used and requires companies to be more transparent in their handling of it. While the law does not go into effect until January 1, 2020, and some operative provisions were delayed until July 1, 2020, the requirements under the CCPA should not be minimized, and companies should take steps to prepare for compliance in 2019 while monitoring ongoing rulemaking.

Who Is Covered?

In general, the CCPA applies to entities conducting business in California that either directly or indirectly control the collection of personal information of residents in that state and meet one or more of the following criteria:

- have annual gross revenues in excess of $25 million, adjusted for inflation;
- derive 50 percent or more of their annual revenues from selling consumers' personal information; or
- annually buy, receive for a commercial purpose, sell or share the personal information of 50,000 or more consumers, households or devices.

What Information Is Subject to the Law?

The CCPA defines personal information very broadly as information about a California resident that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." The CCPA provides a lengthy list of examples that includes standard items such as Social Security, driver's license and passport numbers, as well as items such as purchasing history, internet activity, geolocation data, professional or employment-related information, and inferences drawn about a California resident (that is, using what is otherwise personal information to create a profile of a consumer, such as preferences, intelligence or abilities). Publicly available information is excepted where it is available through government offices.

Issues Businesses Should Consider

The CCPA requires covered entities to disclose, upon request from a consumer, a significant amount of information about that consumer's personal information, including what is being collected, sold or disclosed; the source of that information; the business purposes for collecting or selling it; and the categories of third parties with which the information is shared. The CCPA gives consumers the right to access a copy of their personal information "in a readily useable format that allows the consumer to transmit [the] information from one entity to another entity without hindrance." In effect, this requirement gives consumers a data portability right, since they can migrate their personal information from one service provider to another offering

This article is from Skadden's *2019 Insights*.

Four Times Square
New York, NY 10036
212.735.3000

similar services. Companies also must honor a consumer's request to delete their personal information absent certain defined circumstances.

Implementing processes and procedures to comply with the foregoing requirements — such as being able to provide a consumer with information about their personal data or delete it from the company's systems — can be time-consuming and resource-intensive. Starting a compliance process well in advance of 2020 is strongly recommended.

The CCPA requires that companies provide consumers with the right to opt out of the sale of their personal information through a clear and conspicuous link on the company's homepage titled "Do Not Sell My Personal Information" as well as a link to the relevant privacy policies. For some companies, this will simply mean a change in their user interface. In other cases, this will impact a company's business model, since it likely will result in fewer consumers providing consent. The CCPA forbids companies from discriminating against consumers with respect to prices or services based on their exercise of their rights under the CCPA.

Companies also will need to update their privacy policies, including by describing the consumer's rights under the CCPA and providing a list of categories of personal information collected, sold to a third party or disclosed for business purposes.

Enforcement

Although the CCPA does not provide for a private cause of action (other than in data breach cases), the California attorney general can impose hefty fines for violations that include damages of up to $2,500 per violation if not cured within 30 days. It remains to be seen how California will interpret "per violation." Enforcement actions may not be brought by the attorney general until the earlier of July 1, 2020, or six months after publication of the final regulations.

The CCPA also makes it far easier for consumers to sustain a data breach claim, by not requiring a showing of harm from the incident. Consumers' inability to establish any harm has until now resulted in the dismissal of many data breach cases for lack of standing. It remains to be seen whether this aspect of the law will be challenged.

Will GDPR Compliance Also Satisfy the CCPA?

While some overlap exists between the CCPA and the European Union's General Data Protection Regulation (GDPR) (see "European Data Protection and Cybersecurity in 2019"), they differ in certain key aspects:

- The CCPA's definition of personal information is more extensive than that in the GDPR;
- The CCPA is expected to provide broader rights to request data deletion and includes different exceptions to this requirement;
- The CCPA is expected to provide more power for consumers to access personal information and does not provide all of the exceptions available under the GDPR; and
- The CCPA includes more stringent restrictions on sharing personal information for commercial purposes than does the GDPR.

While companies that have become GDPR-compliant may have an approach to data protection that will be useful in adapting to the CCPA's requirements, GDPR compliance cannot be seen as dispositive for CCPA purposes.

Key Takeaways

Many companies underestimated the time and resources required for GDPR compliance and remained noncompliant when the law went into effect. Companies would be well-served to learn from that experience and begin to implement CCPA compliance programs a year in advance. The challenge companies will face is that CCPA rulemaking is ongoing, and it remains to be seen how some provisions will be interpreted.

Click here for a full list of cybersecurity and privacy-related articles authored by Skadden attorneys in the last year.