MARSH

The CCPA: A Paradigm Shift for US Privacy Law

A new privacy law enacted by California is set to become the most stringent and comprehensive piece of data protection legislation in the United States. The California Consumer Privacy Act (CCPA) takes effect January 1, 2020, giving the California legislature time to refine the law, which it has already done once. Although further changes are expected before its 2020 effective date, the bill represents a major development for privacy rights in the US.

New Rights for California Residents

Under the CCPA, all California residents, referred to as "consumers," will be protected. Further, the CCPA considers any data used to identify an individual, including biometric, commercial, and geolocation identifiers, as "personal information."

The law will give consumers the right to know what personal data is collected, how and why it is being collected, and with whom the data is shared. Consumers are also entitled to access their data, request that it be deleted, and prevent it from being sold to third parties. Businesses, meanwhile, cannot discriminate on the basis of a consumer's request to opt out from having their data sold to third parties.

The CCPA has broad application. The new law will affect any company that collects or processes personal information and has annual revenue of at least $25 million, maintains data of at least 50,000 people, or derives 50% or more of its revenue from selling consumer data.

California's attorney general will enforce the CCPA, but consumers also can bring a private right of action for violations. Non-compliance can result in a penalty up to $7,500 per consumer for intentional violations ($2,500 if unintentional), or between $100 and $750 per violation in a private right of action. Through either route of enforcement, these penalties can quickly compound and grow steep.

"Golden State GDPR," or Something Else?

Comparisons between the CCPA and the EU General Data Protection Regulation (GDPR) are inevitable and, in fact, there are several similarities. Both the CCPA and the GDPR require companies to advise individual consumers of how they collect, use, and share data. The CCPA and the GDPR both also emphasize the value of data encryption and pseudonymization. For consumers, both regimes provide access to their collected data and identify the circumstances when companies can justifiably refuse a data deletion request. Most compellingly, both carry the threat of costly fines and penalties.

Overall, however, the GDPR is more comprehensive and — for now — places more compliance requirements on companies, while the CCPA has fewer enshrined personal rights. For example, while the GDPR gives individuals the right to demand "erasure" of personal data, under the current version of the CCPA, California consumers can only request the deletion of their data. The CCPA also does not provide a separate right to data rectification and does not mirror the GDPR's requirements for subject companies to conduct a data protection impact assessment or appoint a data protection officer.

Additionally, the CCPA may be more forgiving of non-compliance. Companies found to be in violation will have a 30-day window to turn things around prior to the attorney general's office potentially levying a penalty. No such buffer exists with the GDPR, although enforcement is ultimately at the discretion of each EU member state's data protection authority. Still, while the GDPR is more robust overall, the CCPA has some unique characteristics and benefits, such as the private right of action and the ability of California consumers to prevent the resale of their data.

Coverage Availability and Insurability

Most cyber insurers have been noncommittal on whether they will cover CCPA penalties, although so far, some have indicated they will likely take a similar affirmative coverage position as they are taking with the GDPR. However, even if such coverage is provided, whether CCPA penalties are insurable is still an open question. Most policies say coverage applies "where insurable," and California does not have a strong history of allowing punitive measures to be insured.

However, there is cause for optimism. Because the CCPA provides for awards to be assessed *per consumer,* there is a far better chance that penalties under the law will be considered compensatory to individuals rather than punitive to offending companies. This would allow for a better chance for insurability — however, the decision will ultimately depend on how courts and regulators weigh in on the issue.

Suggested Actions for Organizations

While California legislators consider potential refinements to the CCPA, businesses should determine whether they are subject to the law. If a company is subject to the CCPA, it should create a compliance action plan and begin to assess related enterprise risk. This will be a lighter lift for those that have already performed this exercise in preparation for the GDPR.

Companies that are not subject to the CCPA would still be well-served to assess their data collection practices, as there is a strong possibility that other US states may soon pass similar legislation. After all, California's data breach law was, and remains, the standard after which many other US state data breach laws are modeled — and the same could happen with the CCPA in the realm of privacy.

For more information on this topic, visit marsh.com, email the Marsh cyber team at cyber.risk@marsh.com, or contact:

JEFFREY BATT
Vice President, Marsh US Cyber Practice
+1 202 263 7880
jeffrey.batt@marsh.com