California Enacts America's Strictest Data Privacy Statute

by Diane D. Reynolds, Esq.

Diane D. Reynolds

California Governor Jerry Brown (D) signed California Consumer Privacy Act of 2018 into law on June 28, 2018. The statute replaced and nullified a ballot initiative that would have appeared on the November general election ballot and takes effect on January 1, 2020.

The statute applies to any entity that "does business in California" and (a) has annual gross revenues in excess of $25 million dollars; (b) alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or (c) derives 50% or more of its annual revenues from selling consumers' personal information.

Entities that are controlled by and share common branding with a covered business are also covered by the statute. The statute defines "controlled" as ownership of, or the power to vote more than 50% of a business' voting stock; control over the election of a majority of the business' directors or managing members, or the power to exercise a controlling influence over the management of a company and defines "common branding" as a shared name, service mark, or trademark.

The statute is ambiguous as to whether it applies to out-of-state corporations with no contact with California other than maintaining a website or application accessible by California residents. Additional highlights include:

The statute imposes a duty on all covered entities to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information" they possess.

- The statute creates a private right of action under which any consumer whose personal information is subject to unauthorized access and exfiltration, theft, or disclosure as a result of a covered business' breach of this duty to receive the greater of actual damages or statutory damages of $100-$750 for each incident.
- All other provisions of the statute are solely enforceable by the California Attorney General, which prompted the American Civil Liberties Union (which supported the now-nullified ballot initiative's private right of action for all violations) to call the statute "inadequate".
- The statute broadly defines "personal information" to encompass information including but not limited to IP addresses, account usernames, purchasing histories, Internet browsing and messaging histories, biometric data, location information, and employment information.
- The statute requires covered entities to disclose to any natural person residing in California upon request the categories and specific pieces of information it collected from them and the categories of third parties with whom such information is shared. It also requires covered entities to delete any personal information collected from a customer upon his or her request unless retaining such information is necessary in order to serve several enumerated purposes.
- The statute mandates that customers be given the right to opt out of sales of their personal information.
- The statute requires affirmative consent to sell the personal information of any consumer under the age of 16.
- The statute prohibits covered businesses from discriminating against customers who exercise any rights provided by the statute.

Although the statute is ambiguous regarding whether it applies to healthcare providers located in other states that treat patients residing in California or maintain websites or applications accessible in California, New Jersey healthcare providers should consider adopting more robust privacy policies and procedures that comply with the new California statute so that they will not be forced to maintain two sets of compliance policies and procedures if California courts hold that they are subject to the statute with regards to patients residing in California. Further, given New Jersey's progressive, pro-consumer rights legislative history combined with the conceptual parallels of the California bill with the recently enacted European Union General Data Protection Regulation, there is a realistic possibility that similar legislation could be introduced not only in New Jersey, but in other states as well, and, perhaps, at the federal level.

About the Author

Diane Reynolds is Of Counsel and heads the cybersecurity practice at McElroy, Deutsch, Mulvaney & Carpenter, LLP. She can be reached at DReynolds@mdmc-law.com.