SAUL EWING ARNSTEIN & LEHR LLP

Alert

CYBERSECURITY AND PRIVACY PRACTICE

FEBRUARY 2019

AUTHOR

ALEXANDER R. BILUS

REBECCA J. FEUERHAMMER

The California Consumer Privacy Act of 2018 Will Impact Businesses Across the Country – Begin the Compliance Process Now

SUMMARY

In the wake of recent privacy scandals and the recent rollout of the European Union's General Data Protection Regulation (GDPR), California legislators took action to give California consumers more control over their own personal information. On June 28, 2018, California passed Assembly Bill 375 and enacted the California Consumer Privacy Act of 2018, a stringent privacy law that has the potential to drastically affect how businesses across the United States collect and use personal information. On September 23, 2018, Governor Jerry Brown signed SB-1121 into law and amended provisions of the Act. This alert breaks down the key aspects of the Act and its amendments to explain how businesses can continue the compliance process.

What businesses are affected?

The Act applies to any for-profit business that collects the personal information of California residents, that does business in California, and that meets any of the following thresholds: (1) has annual gross revenues of at least $25 million; (2) buys, sells, receives, or shares for commercial purposes the personal information of 50,000 or more consumers, households, or internet-connected devices; or (3) derives 50 percent or more of its annual revenue from selling consumers' personal information. Even a business that is not physically located in California is subject to the Act if it meets these requirements. The Act also applies to certain parent companies and subsidiaries of those businesses, and to service providers that process personal information on behalf of those businesses and to whom the personal information is disclosed.

What data is protected?

The Act covers "personal information," which is defined as information 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. This definition is very broad and covers the following, if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household: personal identifiers (such as name, address, IP address, SSN, or driver's license number), characteristics of protected classifications under California or federal law (such as race, ethnicity, gender, and veteran status), commercial information (such as records of personal property and products or services purchased), biometric information, internet activity information (such as browsing history, search history, and interactions with a website), geolocation data, audio and visual information, employment-related information, education information that is protected under the federal Family Educational Rights and Privacy Act (FERPA), and inferences drawn from this information to create a profile about a consumer reflecting the consumer's preferences, characteristics, and attitudes.

What data is excluded?

The Act does not apply to information publicly available, to medical information governed by the Confidentiality of Medical Information Act, protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the Department of Health and Human Services established pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPPA), information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration or to information governed by the Gramm-Leach-Bliley Act, the California Financial Information Privacy Act, or the Driver's Privacy Protection Act of 1994.

What rights are granted to California residents?

The Act gives the following rights to each California resident:

- the right to request access to the personal information that a business has collected about that consumer;
- the right to request that a business delete the personal information, subject to certain exceptions;
- the right to request that a business disclose to the consumer certain information, including the categories of personal information that the business has collected about the consumer, the categories of sources for that information, the business purpose for the collection or selling of the information, and the categories of third parties with whom the business shares or to whom the business sells the information; and
- the right to direct a business that sells personal information to third parties not to sell the consumer's information (a.k.a. the right to opt out).

These rights of access, deletion and control over a third party's use of personal information are somewhat novel concepts in U.S. law, but they are modeled on the rights recently granted to all European Union residents by the GDPR. This expansion and strengthening of privacy rights in Europe, and now California, portends a possible further growth in privacy rights throughout the rest of the United States.

What must a business do to comply?

The Act imposes a number of obligations on any business that falls within its scope, including the following:

- at or before the point of collecting personal information, inform consumers about the categories of information to be collected and the purposes for which they shall be used;
- respond within 45 days to requests by California consumers to exercise their rights under the Act;
- do not discriminate against a consumer because the consumer exercised any of his or her rights under the Act, including by denying goods or services to the consumer or by charging different prices or rates for goods or services or providing a different level or quality of goods or services (beyond any difference that is reasonably related to the value provided to the consumer by the consumer's data);
- disclose certain information in its online privacy policy or on its website;
- train its employees who are responsible for handling consumer inquiries about the business' privacy practices or compliance with the Act;
- execute contracts with its service providers to prohibit those providers from retaining, using or disclosing the personal information for any purpose other than for the specific purpose of providing the services to the business; and
- implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information.

How and when will the Act be enforced?

The California Attorney General is authorized to bring a civil action in the name of the people of the State of California for an injunction and a civil penalty of not more than $2,500 for each violation of the Act, or $7,500 for each intentional violation of the Act. More significantly, the Act also creates a private right of action for any California consumer if the consumer's nonencrypted or nonredacted personal information is subject to unauthorized access or exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices. The consumer can recover damages and seek injunctive or declaratory relief if certain requirements are met. Among other requirements, prior to bringing any action on an individual or class-wide basis for statutory damages of $100 to $750 per incident, a consumer must first provide 30 days' written notice to the business to give the business an opportunity to cure the violation. Unlike the GDPR, the CCPA has no cap on the maximum amount of damages or fines that can be imposed on a business—thus, the CCPA arguably presents a greater risk to businesses that fail to comply.

The Act goes into effect on January 1, 2020 (with certain provisions going into effect on July 1, 2020), giving businesses time to complete the compliance process. Importantly, however, the Act includes a twelve-month "look back" period for customer requests, so customers will be able to obtain information about a business' use of their personal information going back to January 1, 2019. We recommend that all businesses that may be impacted by the Act seek legal counsel to help determine if they are covered by the Act and, if so, to assist with drafting the privacy notices, policies and procedures, and contracts that are required by the Act.

This Alert was written by Alexander R. Bilus, co-chair of the Cybersecurity and Privacy Practice, and Rebecca J. Feuerhammer, an associate. Alexander can be reached at (215) 972-7177 or alexander.bilus@saul.com. Rebecca can be reached at (215) 972-7843 at rebecca.feuerhammer@saul.com.