LOCKE LORD® QUICK Study
Privacy & Cybersecurity Practice
July 5, 2018

Dropping Another Stone in the Pond?

California's New Consumer Privacy Act

By: Ted Augustinos and Molly McGinnis Stine

California may have again taken the privacy protection lead among U.S. jurisdictions with the Governor's signing on June 28, 2018 of the California Consumer Privacy Act of 2018 (AB 375) (the "Act"). Privacy and security professionals will remember the ripple effect of California's first-in-the-nation data breach notification statute in 2003, which was ultimately taken up with variations throughout each of the United States, resulting in a patchwork of state data breach requirements that have been challenging and expensive for businesses to address. With the last of the states only just now on board with some form of data breach notification requirement, has California dropped another stone in the pond?

Unanimous Compromise

The Act unanimously passed both houses of the California legislature as a compromise measure intended to undercut an even more stringent and onerous ballot initiative of the same name scheduled for the November elections. The Act will become effective in January 2020, and may well be subject to further amendments between now and then.

European Inspiration; Broad Application

The new California law was clearly inspired by the privacy and data security protections of the General Data Protection Regulation ("GDPR") of the European Union, which took effect on May 25, 2018. It follows several themes of the GDPR, including consumer rights (i) to know what personal information is collected about them, (ii) to prevent the sale of personal information, (iii) to know categories of personal information (if not the actual data) shared with third parties, and (iv) to be forgotten by requiring deletion of personal information. While the GDPR uses the term "personal data" and California uses "personal information," both terms are defined broadly to include essentially any information that identifies or is reasonably identifiable of an individual. Companies that will be subject to both the Act and the GDPR will, however, need to consider several nuances in the definitions. For example, the Act excludes information that is publicly available from its definition of personal information, while the GDPR does not have such an exclusion from the definition of personal data.

Who is Subject? Who is Protected?

The Act applies to any business that collects personal information about California consumers if it does business in California and meets one of the following thresholds:

- Annual gross revenues in excess of $25 million;
- Annually buys, receives for commercial purposes, sells, or shares for commercial purposes, personal information of 50,000 or more consumers, households or devices; or
- 50 percent or more of annual revenues are derived from selling consumers' personal information.

Consumer includes any identifiable natural person who is a California resident.

What is Required?

As noted above, many of the themes of the Act track the GDPR. More specifically, business that collect personal information from California consumers must prepare now for the following requirements to become effective in 2020:

- Notice Requirement: At or before the time of collecting personal information, the business must provide notice of the categories of personal information to be collected, and the purposes for which they will be used.
- Disclosure Requirements: Upon request of a consumer, the business must disclose
  - the categories and specific pieces of the consumer's personal information the business has collected;
  - the categories of sources from which personal information is collected;
  - the business or commercial purpose for collecting or selling personal information;
  - the categories of third parties with whom the business shares personal information.
- Delivery of Personal Information: Upon request of a consumer, up to twice in a 12-month period, the business must deliver to the consumer all of the consumer's personal information collected.
- Right to be Forgotten: Each business must notify consumers of their right to request the business to delete all of the consumer's personal information. Certain exceptions permit the business to retain personal information for specific purposes.
- Non-Discrimination: With limited exceptions, businesses are prohibited from discriminating against a consumer because the consumer exercised any of the consumer's rights under the Act, including denying goods or services, charging different prices, providing a different level of quality of goods or services, or suggesting that the consumer will receive a different price or level of quality of goods or services.

Private Right of Action, in Some Circumstances

Under certain circumstances, a consumer can pursue a private right of action if the California Attorney General does not pursue enforcement of the Act and the consumer's personal information was subjected to unauthorized access, exfiltration, theft, or disclosure as a result of a business's violation of the duty under the Act to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the information. A consumer can sue over a violation and recover the greater of actual damages or statutory damages of between $100 and $750. The Act gives a business a 30-day period to cure the violations identified by the consumer. If the business confirms in writing that the situation has been corrected and will not recur, no suits for statutory damages can occur. In addition, the consumer must advise the California Attorney General within 30 days of a lawsuit. The Attorney General then has 30 days to either supersede the private action and pursue its own action or to permit the private action to proceed. It may be the topic of further legislative discussion whether the Act requires a consumer to demonstrate actual injury to file suit or whether an allegation of a violation of the Act involving the consumer's personal information is sufficient. On a related note, the Act bars any contractual limit on a consumer's right to recovery, which could prohibit contracts requiring arbitration as an exclusive form of dispute resolution.

What Should Businesses Do Between Now and 2020?

As noted above, amendments between now and the Act's effective date are possible, but businesses need to start planning now. First, if the history of breach notification laws is any indication, one can expect that other states will follow California's lead in adopting privacy protections that echo the themes established by the GDPR. Second, given the size of California's economy, many businesses will be subject to the requirements of the Act, whether or not other states adopt their own privacy legislation.

Given the nature and extent of the Act's requirements, compliance will take a lot of planning and effort for many businesses. Businesses that collect personal information from California consumers should take the following steps in preparation for the effectiveness of the Act:

- *Collection of personal information.* Inventory how and from whom personal information is collected.
- *Use of personal information.* Catalogue all of the current and intended uses for personal information.
- *Sale and Sharing of personal information.* Identify all parties to whom personal information is sold, and with whom personal information is shared.

- *Map personal information held by the business and its service providers.* If consumers exercise their right to provide personal information collected by the business, or their right to be forgotten, the business will need to know where the information is located.
- *Develop policies and protocols for meeting the requirements of the Act.* Businesses will need to be organized in order to comply with requests from consumers to provide requested disclosures, or to delete personal data.
- *Review safeguards for protecting personal information.* Given the private right of action and the potential for Attorney General enforcement, in the event of a breach of the confidentiality or security of personal information, businesses should review their safeguards and make appropriate adjustments to protect personal information and mitigate the risk of a breach that could give rise to litigation or enforcement.

For more information on the matters discussed in this *Locke Lord QuickStudy*, please contact the authors.

Ted Augustinos | 860 541-7710 | ted.augustinos@lockelord.com
Molly McGinnis Stine | 312-443-0327 | mmstine@lockelord.com