LOEB & LOEB LLP

Privacy

JULY 2018

California Passes Expansive New Privacy Law

Just as businesses were starting to catch their breath following the implementation of the General Data Protection Regulation, consumer privacy law has again changed dramatically with the passage of the California Consumer Privacy Act of 2018 on Thursday. The law was passed without opposition, having been rushed through the legislature in order to avoid a November ballot initiative that would have imposed even stricter regulations. The act provides consumers with several new rights, including the right to require the deletion of their data, to request disclosures about how information is collected and shared, and to instruct a company not to sell their data.

The law will likely change between now and the 2020 implementation, as the short time in which it was passed left inconsistencies and ambiguities that many different groups are already working to fix. While the basics of this law will receive significant mainstream media attention, there are several practical questions for businesses to consider now.

Does the Law Apply to My Company?

California has historically taken an expansive view of the reach of its laws. If your website is used by California residents, California regulators likely will take the position that the law applies to your company's collection of information through that website. That said, the law does not apply unless your business (1) has $25 million-plus in annual revenue, OR (2) derives 50 percent or more of its revenues from selling consumer data, OR (3) "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." The law applies to offline as well as online businesses that meet these thresholds, so many retailers and other traditional businesses will be affected.

What Is "Personal Information"?

As in the GDPR, the definition of "Personal Information" is quite expansive, meaning 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 includes IP addresses and even inferences drawn from these data to create a profile about a consumer's preferences, behaviors or characteristics. This also includes geolocation information and internet activity information, including browsing history and a consumer's interaction with a site or an advertisement.

Is My Company "Selling" Consumer Information?

While many of the obligations under the law are tied to the selling of consumer information, the law defines "sale" very expansively, to include mere disclosure for monetary or other valuable consideration.

When Is the Law Effective?

January 1, 2020. We anticipate that the law may change between now and the implementation date, so we will monitor for any material revisions. Federal legislation also could supersede all or parts of this law prior to January 1, 2020.

In General, What Is My Company Required to Do?

Even companies that took the significant steps required to be in compliance with the GDPR will have work to do ahead of the January 1, 2020, implementation date Companies that have not dealt with the GDPR will likely have to make significant efforts, so it is important to begin planning soon. Below is a summary of some of the key requirements.

- Before collecting personal information, tell consumers the categories of personal information you collect and the purposes for which it will be collected. You must also inform consumers of their right to have their personal information deleted.
- Twice per year, consumers will have the right to request that a business provide them with details relating to the personal information the business has collected about them. This information must be provided within 45 days of the consumer's request. You must make available to consumers two or more designated methods for submitting such requests, including a toll-free telephone number and a web site address. Specifically, following receipt of a verifiable request, the consumer is entitled to know:
  - The categories of personal information the business has collected about that consumer.
  - The categories of sources from which the 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.
  - The specific pieces of personal information the business has collected about that consumer.
  - The categories of personal information about the consumer that the business sold and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold.
  - The categories of personal information that the business disclosed about the consumer for a business purpose.
- Ensure that your privacy policy informs consumers of the categories of personal information to be collected and the purposes for which the categories of personal will be used. Your privacy policy must also describe a consumer's rights to make the information request described above and include a list of the categories of personal information the business has sold or disclosed about consumers in the preceding 12 months. The privacy policy should be updated at least every 12 months.
  - Companies that may have just revised their privacy policies for the GDPR may need to revise them again before the law takes effect in order to incorporate the notices required in California. Companies will have to consider whether they will offer the same rights to consumers outside of California or create two different privacy policies.
  - Companies that have not already established processes to accommodate consumer requests related to data under the GDPR will also have to develop ways to verify requests are legitimate and provide information to consumers or delete data on request.
- Delete personal information upon a consumer's request (and direct our service providers to do the same); except under limited circumstances that include the following:
  - Where it is necessary to (a) complete the transaction, (b) provide goods/services to the consumer, (c) perform a contract between the parties; (d) comply with a legal obligation; and (e) detect and address security incidents and repair errors that impair intended functionality.
- Implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information.

- Ensure your vendors responsible for handling consumer inquiries are aware of the law's requirements.
- Businesses that sell personal information to third parties must provide a clear and conspicuous link on the business' internet home page, titled "Do Not Sell My Personal Information," to an internet web page that enables a consumer to opt out of the sale of the consumer's personal information.
  - If a consumer opts out of having his or her data shared, the company cannot discriminate against that consumer. However, the law does not prohibit a business from charging a consumer a different price, or from providing a different level or quality of goods or services to the consumer, if that difference is related to the value provided to the consumer by the consumer's data.
- Opt-in consent is required before selling information relating to individuals 16 years of age and under. More specifically, the law provides that a business cannot sell the personal information of a consumer if the business has actual knowledge that the consumer is younger than 16, unless the consumer has affirmatively authorized the sale (or, for consumers less than 13 years old, the consumer's parent or guardian has affirmatively authorized the sale).

What Happens if We Violate the Law?

- The law provides for a private right of action and statutory damages of between $100 and $750 per consumer for data security incidents that occur as a result of the "business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." Intentional violations of the act are subject to a civil penalty of up to $7,500 for each violation.
- Before a consumer can bring an action for statutory damages under the law, the business has to be given a 30-day period to cure the violation, and the state attorney general must be given the option of pursuing the case.

Finally, keep in mind that the foregoing is just a summary of a complicated law that remains subject to potential revisions prior to the January 1, 2020 implementation date. The privacy and data security team at Loeb & Loeb is available to answer any questions about compliance with this new law.