Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

California May Pass Its Own GDPR

By **Purvi Patel and Alexandra Laks** *(May 17, 2018, 12:18 PM EDT)*

Purvi Patel

Alexandra Laks

While companies are focusing on compliance with the EU's General Data Protection Regulation requirements, Californians will be given the option to impose a sweeping, GDPR-like privacy regime that also deserves attention. On May 3, 2018, proponents of the California Consumer Privacy Act announced they had collected the signatures needed to qualify the act for the Nov. 6, 2018 ballot.

If approved by voters in November, the California Consumer Privacy Act would require businesses to disclose the categories of personal information they collect, sell or share about California consumers, and gives consumers a right to say "no" to the sale of their information. The act would also allow consumers to sue for violations (which include data breaches resulting from failure to maintain "reasonable security procedures and practices") without suffering any loss of money or property, and would impose stiff penalties for noncompliance.

The proposed act is far-reaching. It covers virtually any and all information a business has about a consumer and reaches across all industries and business practices. If passed, the act would impose significant compliance challenges, burdens and costs, and greatly increase the risk of litigation. Below, we provide further information regarding some of these new burdens and obligations, including timing and steps for implementation.

Businesses and Information Covered

The act would apply to entities doing business in California if they meet one of the following thresholds: (1) has annual gross revenues in excess of $50 million; (2) annually sells personal information of 100,000 or more consumers or devices; or (3) derives 50 percent or more of its annual revenue from selling consumer personal information.

The act covers "personal information," which it defines broadly as any information that "identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device."[3] This definition includes, but is not limited to, 12 enumerated categories of information about consumers and any minor children of the consumer.

While some of the enumerated categories are expected — identifiers (like name, address, email, Social Security or driver's license number), biometric data, or professional or employment-related information — the act expands far beyond traditional notions of personal information. It includes, for example, "commercial information," which encompasses products or services provided, obtained, or considered, as well as "other purchasing or consuming histories or tendencies." It also includes Internet activity, such as browsing or search history or a consumer's "interaction" with a website, application, or advertisement. The definition of PI also vaguely extends to "inferences drawn" from any of the categories of PI specifically enumerated.

Act Requirements

The act seeks to create the following consumer privacy "rights":

"Right to Know"

Upon request by a consumer, businesses must disclose the categories of PI that the business has, within the year preceding the request: (1) collected; (2) sold to a third party; and/or (3) disclosed to another person for a business purpose. Consistent with its expansive scope, the act broadly defines collecting, selling, and disclosing for a "business purpose" to encompass virtually all aspects of a business's interaction with — and use of — consumer PI:

- If a business buys an email or address list from a direct-mailing-list broker, that information would need to be listed as information "collected."

- If a business shares customer purchase records with a data cooperative in exchange for access to other consumer PI the cooperative has, that information would need to be listed as information "sold," and depending on what the business receives from the co-op, as information "collected."

- If a business provides a consumer's account or transaction information to a third-party customer-support provider or to a third party for processing credit card transactions, that information would need to be listed as information "disclosed for a business purpose."

For businesses that have sold or disclosed the requesting consumer's PI, the business must also provide accurate names and contact information for the receiving parties.

To facilitate consumer requests for information, the act would require businesses to make available two or more designated methods to ask for the information. At a minimum, these methods must include a toll-free number and, if the business has a website, a website address. Businesses would be required to respond in writing within 45 days of a request. These reports would need to be provided free of charge.

In addition, a business must disclose certain information about the act online, including, if applicable, in its online privacy policy or in any California-specific description of consumers' privacy rights. This information, which must be updated at least once a year, includes (1) a description of rights under the act, and (2) a list of categories of PI collected, sold to a third party, or disclosed for business purposes.

Right to "Say No"

Businesses must give consumers the right to opt out of the sale of personal information. The act requires a "clear and conspicuous" link on the business's homepage, titled "Do Not Sell My Personal Information." If the business has a separate page for California consumers and takes reasonable steps to direct California consumers to that page, the business does not have to put the "Do Not Sell" link on its homepage. Any information collected in connection with a consumer's opt-out request may only be used for purposes of complying with the opt-out request.

Right to Sue for Violations of the Act

The act provides a private right of action for violations of its provisions in the amount of $1,000 per violation (or up to $3,000 for willful violations) of statutory damages or actual damages, whichever is greater. The act is silent, however, on what constitutes a "violation" — i.e., in the context of a delayed response to a request, for example, whether a "violation" is a single failure to respond per person or whether that failure is multiplied per category of PI or per day, or, in the context of an incomplete disclosure, whether a "violation" is the errant disclosure itself or the category or categories of PI excluded.

A violation of the act alone is enough for an injury-in-fact, meaning the plaintiff need not have suffered any loss of money or property to have standing to sue. The act also provides for public enforcement by the California attorney general or district attorney (as well as, under certain circumstances, a county counsel, city attorney, or city prosecutor), with civil penalties of up to $7,500 for each violation. Finally, the act provides a "whistleblower" enforcement mechanism that would allow individuals to stand in the shoes of the AG to seek civil penalties for violations.

Notably, there is no "good faith" compliance or "bona fide" error or mistake exception. There is, however, a non-California "exemption" that provides that the obligations imposed by the act shall not restrict a business's ability to collect and sell consumer PI so long as every aspect of the commercial conduct takes place outside of California.

Right to Sue for Data Breach

The act also creates new liabilities for security breaches involving consumers' PI (as defined in California's data breach notification law, California Civil Code § 1798.82). A business that has suffered a data breach and failed to implement and maintain "reasonable security procedures and practices" to protect the disclosed PI will be deemed to have violated the act, opening the business up to the act's statutory penalties. The act specifies that consumers, law enforcement, or whistleblowers may sue for a data breach.

The potential exposure could be enormous if a "violation" is the number of individuals and/or records impacted as opposed to the breach incident itself. Assuming a breach of one million consumer records, if a defendant is found liable under the act, the statutory damages from a consumer action could amount to $1 billion.

This provision appears designed to overcome court decisions finding that consumers lack standing to sue for data breaches where they cannot demonstrate actual harm or a likely threat of future harm. The act would likely lower the bar for standing in data breach cases, thereby making dismissal more difficult and potentially raising the "headline" number for private consumer and law enforcement data breach settlements.

Timing and Steps for Implementation

If passed, the act will be effective immediately on the day following the election — Nov. 7, 2018. With respect to the consumer PI requirements, however, the act provides for a nine-month grace period from the Nov. 7 effective date, and would apply only to PI collected on or after Aug. 7, 2019.

The act also requires that, if the California attorney general determines it necessary to adopt implementing regulations, he do so within six months of the act's adoption. The act further provides that the AG may adopt "interim regulations" without complying with the Administrative Procedure Act (which requires notice of rulemaking, a 45-day comment period, and public hearings if requested), and that those interim regulations will remain in effect for 270 days unless superseded by regulations adopted pursuant to the APA.

Takeaway

If a business is within the scope of the California Consumer Privacy Act, the act reaches virtually any and all information that a business has about its customers as well as any and all ways that a business interacts with, or uses, that information.

Planning for compliance will take time, resources and careful consideration. As an initial step, businesses should thoroughly review what information they collect about California consumers. Given the broad scope of information covered by the act, it is unlikely that businesses are maintaining all relevant information centrally, and it will be important to canvas and collaborate across departments and divisions. Second, businesses should organize, in a single place, information regarding the sale or disclosure of any consumer PI to third parties. Depending on the purpose associated with collecting, selling, or sharing consumer PI, it may be necessary to assess the ongoing need to do so as consumer privacy issues continue to occupy legislatures and the courts.

This act is symptomatic of a growing trend toward regulating businesses' collection and use of consumer personal information in the name of privacy. That the act garnered nearly twice the signatures required to qualify for the ballot suggests its focus on privacy will resonate with voters. Businesses need to stay abreast of proposed privacy legislation, and be prepared for any changes to come.

Purvi G. Patel is a partner and Alexandra Eve Steinberg Laks is an associate at Morrison & Foerster LLP.