California Enacts Sweeping Privacy Law; Will Other States Follow?

Dana B. Rosenfeld, Alysa Z. Hutnik

June 29, 2018

On June 28, 2018, Governor Brown signed into law the "California Consumer Privacy Act of 2018." The legislation was a compromise to avoid a ballot initiative that was more closely modeled after the European Union's General Data Protection Regulation. This Act is scheduled to go into effect on January 1, 2020.

Which Businesses and Personal Data Are Subject to the California Law?

The Act applies to businesses:

- that collect consumers' personal information, or on whose behalf such information is collected, and
- that do business in California and either, (1) have gross revenues over $25 million; (2) annually buy, receive, sell, or share personal information from at least 50,000 consumers, households, or devices; or (3) receive at least 50% of annual revenues from selling consumers' personal information.

"Personal information" is broadly defined to include any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be directly or indirectly tied to a particular consumer or household. Some examples include a consumer's real name, unique identifier or alias, online identifier IP address, email address, account name, government-issued identification number, professional or employment-related information, biometric information, commercial information (personal property records or products purchased, obtained, or considered), Internet browsing or search history, geolocation data, audio, electronic, visual, thermal, olfactory or similar information, and inferences drawn from any personal data to create a profile reflecting the consumer's preferences, characteristics, behavior, etc. The term excludes publicly available information.

Overview of California Privacy Law Requirements

Right to Request Information Disclosure: A consumer has a right to request from a business that collects or sells personal information about the consumer the categories and specific pieces of personal information collected about such person. Upon a verifiable consumer request, businesses must disclose, free of charge, the categories of personal information, sources of that information, the business reason for collecting the information, the categories of the third parties the company shares the information with, and the specific pieces of information the company has collected. This

disclosure may be provided electronically (in a portable form, and where possible, in a readily usable format) or by mail. A business is not required to provide such personal information more than twice in a 12-month period.

Retention: Businesses are not required to retain any personal information if collected for a one-time transaction, and in the ordinary course, do not sell or re-identify or link the information in a manner that would render it personal information.

Right to Be Forgotten: Businesses are required to delete any personal information they have collected from a consumer if the consumer requests the deletion, unless the company is using the information for certain specific purposes, such as to complete a requested transaction, information security, for free speech purposes, peer-reviewed research, for solely internal purposes aligned with consumer expectations based on the relationship with the business, or to comply with a legal obligation.

Right to Consent as to the Sale of Consumer Information: Businesses that sell a consumer's personal information must give the consumer an opportunity to **opt out** of having their information sold and inform the consumer of this right. A business cannot sell the personal information of youth between the age of 13 and 16 without the person's affirmative **opt in** of the sale, and of the parent's affirmative **opt in** for the personal information of children under the age of 13.

Right Not To Be Discriminated Against for Exercising Privacy Rights: Businesses cannot discriminate against consumers who exercise their rights under the law by denying them goods, charging them different prices or suggesting that they will charge consumers different prices, or giving them a different level or quality of goods. A business *can*, however, charge a consumer a different price or give them different goods if that difference is reasonably related to the value the consumer would receive based on the consumer's data. Businesses can also offer consumer financial incentives for the collection, sale, or deletion of personal information or offer the consumer a different price, rate, level, or quality of goods or services if that difference is directly related to the value that the consumer would receive based on their data, the business gives the consumer notice of the financial incentives, and the consumer provides an opt in after disclosure of the material terms of the program and retains the ability to revoke consent at any time.

What Else Does the California Law Require Businesses to Do?

Give Consumers Options for Making Requests: Businesses are required to provide the consumer with at least two methods for submitting information requests, including a toll-free number, and a website address, if applicable.

Make Disclosures Within 45 Days, Free of Charge: Businesses must provide the consumer with the information requested in writing within 45 days after the business receives a verifiable consumer request. If necessary, this period can be extended once, by an additional 45 days. The disclosure must provide all information requested that the business has collected within the previous 12 months of receiving the request. Depending on the complexity and number of requests, a business may have up to 90 additional days to respond, although the business must inform the consumer of the extension and reason for the extension within 45 days of receiving the request.

Privacy Policy Disclosures: Businesses must describe a consumer's rights in its privacy policy and provide at least one way the consumer can submit requests. Businesses must also include additional information in their policies depending on how they use the consumer information.

- *If the business shares personal information with third parties:* Businesses must disclose a list of the categories of personal information that they have collected about consumers in the last 12 months, referencing the specific categories of information collected and of the third parties with whom the businesses share the information.
- *If the business sells personal information to third parties:* Businesses must provide a list of personal information that they have sold in the past 12 months based on the categories specified in the law, or disclose that they have not sold such information, if they have not.

Website Opt Out Link Notification: Businesses that sell consumer personal information must provide a clear and conspicuous link on the homepage of their websites that states "Do Not Sell My Personal Information" to allow a consumer to opt out of the sale of the consumer's personal information, whether or not the consumer creates an account with the business. Businesses must also include this link in their privacy policies. Businesses cannot sell the personal information of a consumer that has opted out of the sale, but the business can request the consumer to authorize the sale after 12 months. Any personal information the business collects for the purpose of opting out must only be used for that purpose. If the Attorney General so regulates, the consumer may have another person opt out of the sale on the person's behalf.

Training: Businesses must ensure that their employees handling such consumer inquiries are informed of the law's requirements.

Limited Use of Verification Information: Any information that a business collects to verify a consumer's identity should only be used for that purpose.

Exposure for Violations of the California Law

Consumers Have a Private Right of Action for Data Breaches: If a consumer's nonencrypted or nonredacted personal information is breached and exfiltrated, stolen, or disclosed as a result of the business not implementing reasonable security procedures and practices, then the consumer can bring a civil action against the business for the greater of damages between $100 and $750 per consumer per incident or actual damages, or injunctive or declaratory relief. The Act does require that the consumer give the business 30 days' written notice and the ability to cure the violation and inform the consumer, in writing, of the cure before initiating an action for statutory damages or a class action. However, if the business breaches the written notice, the consumer can then initiate an action to enforce the written statement and pursue statutory damages for both breaches of the statement and any violation based on the consumer's original notice. The consumer must also notify the Attorney General within 30 days of filing the action. Within 30 days, the Attorney General can either (1) inform the consumer that the office intends to prosecute the violation itself, and do so within six months, or (2) refrain from acting and allow the consumer to proceed with his or her action.

Willful Violations: A business that intentionally violates the Act is subject to $7,500 for each violation.

Third-Party Liability: If a business discloses information to a service provider, and that third party violates the Act, the business will not be held liable if it did not have actual knowledge or reason to believe that the service provider intends to commit the violation.

Arbitration/Class Action Waiver Limitations: The Act also provides that any terms that purport

to waive or limit a consumer's rights under the Act, including remedies or enforcement options, shall be deemed void and unenforceable.

Other Notable Exemptions: The Act contains several exemptions for personal information governed by certain federal laws, such as HIPAA, GLBA, FCRA, and the Driver's Privacy Protection Act, or where a business's compliance with the law would void an evidentiary privilege.

* * *

Although the law may change between now and its 2020 implementation date, California once again has thrown the gauntlet down with an expansive take on consumer privacy. If past is prologue, other states are sure to follow, raising questions about the feasibility for companies with nationwide practices to meet different and conflicting privacy federal and state standards. Notably, the Federal Trade Commission will be holding hearings on the harmonization and interpretation of federal and state laws addressing unfair and deceptive practices (which include privacy). California's new law may well be a key topic raised on this point.