Published on *The National Law Review* https://natlawreview.com

New Law Expands California Consumer Privacy Rights and Protections

Article By:

Anjali C. Das

California takes the lead once again by enacting stricter privacy laws designed to protect consumers' rights over their personal data. In November 2020, the California Legislature passed the Consumer Privacy Rights Act (CPRA or the Act), which goes into effect on January 1, 2023. The CPRA amends and expands the existing California Consumer Privacy Act (CCPA). Failure to comply with the new law may subject companies to enforcement actions and stiff fines and penalties by regulators.

Overview: California Privacy Rights Act

The CPRA affords greater protections to California consumers with respect to the collection, use and sale of their personal information (PI). In addition, the CPRA imposes more onerous requirements on businesses to disclose their activities involving consumer data, and provides steps that consumers can take to restrict the use of their data. Businesses are required to implement reasonable security measures to protect PI. To the extent they share consumer data with third-party vendors or contractors, businesses must enter into agreements that require these downstream parties to comply with the Act as well. The CPRA creates a new state agency, the California Privacy Protection Agency, which, in addition to the California Attorney General and District Attorneys, can prosecute violations of the Act.

Organizations Subject to the Law

The Act does not apply only to California-domiciled organizations. The Act generally applies to any organization that conducts business in the state of California, collects or processes PI, *and* meets *one or more* of the following criteria:

- Controls or processes personal data of 100,000 California consumers or households annually
- As of January 1 of the calendar year, had annual gross revenue in excess of $25 million in the preceding calendar year
- Derives 50 percent or more of its annual revenue from selling or sharing consumers' PI.

The processing of personal data includes the collection, use, storage, disclosure, analysis, deletion or modification of personal data.

Notably, certain organizations are exempt from compliance with the Act, including government agencies, financial institutions subject to the Gramm-Leach-Bliley Act (GLBA), entities subject to the Health Insurance Portability and Accountability Act (HIPAA), and nonprofit organizations.

Protected Personal Information

The Act broadly defines “personal information” to include any information that identifies, relates to, describes, could reasonably be associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

Examples of personal data include unique personal identifiers such as names and addresses; commercial information related to the consumer; biometrics; internet or other electronic network activity information; geolocation data; audio, electronic, visual, thermal, olfactory or similar information; professional or employment-related information; education information not publicly available; and even inferences drawn from any of the information identified to create a profile about a consumer.

The Act also distinguishes “sensitive personal information” (SPI), which includes specific categories of data such as government identifiers (e.g., social security numbers and driver’s licenses); financial account and login information (such as a credit or debit card number together with login credentials); precise geolocation; race, ethnicity, religious or philosophical beliefs; union membership; content of nonpublic communications (mail, email and text messages); genetic data; biometric or health information; and sex life or sexual orientation information.

California Consumers’ Data Protection Rights

The Act recognizes broad data protection rights over consumers’ personal information, including:

- Right to delete PI
- Right to correct inaccurate PI
- Right to know what PI is being collected (including categories of PI collected; sources from which PI is collected; commercial purpose for collecting, selling or sharing PI; categories of third parties to whom PI is disclosed; and the specific pieces of PI about the particular consumer)
- Right to know what PI is sold or shared, and the recipient
- Right to opt out of the sale or sharing of PI
- Affirmative authorization required for the sale or sharing of minors’ PI
- Right to limit the use and disclosure of SPI.

To enable consumers to exercise their data protection rights, a business is required to make

available two or more means for submitting requests, including, at a minimum, a toll-free number. A business that operates exclusively online and has a direct relationship with the consumer is required to provide only an email address. If the business maintains an internet website, requests also can be submitted via the website.

Once a business receives a verifiable request by a consumer to exercise one or more of their rights under the Act, the organization is required to respond in writing within 45 days, free of charge. This time period may be extended once by an additional 45 days with timely notice to the consumer. The disclosure of required information to a consumer shall cover the preceding 12 months from the date of receipt of the request. However, a consumer may request information beyond the 12-month period only with respect to PI collected on or after January 1, 2022. A business is not obligated to provide information to the same consumer more than twice in a 12-month period.

Businesses' Disclosure Obligations

Pre-Collection Disclosure Obligations**:** A business that collects (or controls the collection of) consumers' PI must disclose the following information to consumers at or prior to the point of collection:

- Categories of PI or SPI to be collected
- Purposes for which the PI or SPI are collected or used
- Whether the PI or SPI will be sold to or shared with third parties
- Length of time PI or SPI will be retained.

Privacy Notice**:** Businesses also should disclose the following information to consumers in an online Privacy Policy or on its website:

- Description of California consumers' privacy rights under the Act
- Two or more methods for consumers to submit requests to exercise their rights
- List of the categories of PI collected, sold or shared in the preceding 12 months
- Categories of sources from which PI is collected
- Business or commercial purpose for collecting, selling or sharing PI
- Categories of third parties to which PI is disclosed.

If the business has not sold, shared or disclosed consumers' PI in the preceding 12 months, the business should state this fact.

Opt-Out Mechanisms for Selling or Sharing PI**:** A business that sells or shares consumers' PI or uses or discloses consumers' SPI shall provide one or more of the following methods for consumers to opt out of the sale or sharing of their PI and to limit the use or disclosure of their SPI:

- A clear and conspicuous link on the internet homepage titled "**Do Not Sell or Share My Personal Information.**"
- A clear and conspicuous link on the internet homepage titled "**Limit the Use of My Sensitive Personal Information.**"
- A single, clearly labeled link on the internet homepage that easily allows consumers to opt out of the sale or sharing of their PI and to limit the use or disclosure of their SPI.
- An opt-out preference signal sent with the consumer's consent to a specified platform, technology or mechanism whereby consumers can opt out of the sale or sharing of their PI and limit the use of their SPI.

Vendor Contracts Limiting the Use of PI

Businesses that disclose a consumer's PI to a third-party service provider (contractor) for purposes of processing the data must enter into a binding written contract with the third party that sets forth the following conditions and limitations on the use of PI:

- Prohibits the contractor from selling or sharing the PI
- Prohibits the contractor from retaining, using or disclosing PI for any purposes other than the stated business purpose specified in the contract
- Provides a certification by the contractor that it will comply with the foregoing restrictions and limitation on the use of PI
- Permits the business to monitor the contractor's compliance with the contract terms, including ongoing manual reviews; automated scans; regular assessments, audits or other technical and operational testing at least once every 12 months
- Grants the business the right to take steps to stop and remediate the unauthorized use of PI.

If the contractor engages any other third party (sub-contractor) to assist in processing PI, the contractor must notify the business. The contractor will enter into a binding written contract with the sub-contractor that requires the latter to abide by the same restrictions imposed on the contractor.

Consumers' Private Right of Action for Security Breaches of PI

Any consumer whose PI is subject to unauthorized access, exfiltration, theft or disclosure as a result of a business's violation of a duty to implement and maintain reasonable security practices and procedures may institute a civil action to recover the damages and obtain injunctive or declaratory relief. Recoverable damages are the greater of actual damages or up to $750 per consumer/per incident. Suits may be initiated on an individual or class-wide basis. However, prior to filing suit, the claimant must provide a business with 30 days' notice and an opportunity to cure the alleged violations. Notably, the implementation of reasonable security practices and procedures following a breach does not constitute a "cure" under the Act.

Regulatory Enforcement

Violations of the Act may be enforced by the California Attorney General as well as the California Privacy Protection Agency (Agency). Organizations that are found liable under the Act may be required to pay administrative fines ranging from $2,500 to $7,500 for each violation. Such fines will be deposited into the Consumer Privacy Fund, designed to offset any costs incurred in enforcement actions by state courts, the Attorney General and the Agency.

The Agency may investigate possible violations of the Act on its own initiative or pursuant to a complaint by a consumer. The Agency is required to notify a business of a suspected violation of the Act at least 30 days prior to the Agency's consideration of the alleged violation. The notice shall provide a summary of the evidence and inform the business of its right to participate in any proceeding held by the Agency for the purpose of determining whether probable cause exists for alleged violations of the Act.

If the Agency makes a finding of probable cause, it is required to hold an administrative hearing in accordance with the Administrative Procedures Act. If, following the hearing, the Agency determines that a violation has occurred, the Agency may issue a cease and desist order and/or levy an administrative fine.

The Agency also may bring a civil action and obtain a judgment in state court.

Conclusion

Companies should reassess their compliance with the CCPA amendments imposed by the CPRA, which take effect January 1, 2023, to mitigate the risk of potential civil liability, enforcement actions and administrative fines. In particular, companies should:

- Identify the type of PI (including sensitive data) collected from consumers
- Implement and maintain reasonable security measures to protect PI
- Identify third parties with which they share or to which they sell PI
- Review vendor contracts and restrictions on the use of PI
- Audit their vendors for compliance
- Review their own Privacy Notices
- Test their procedures for responding to consumers who exercise their privacy rights.

National Law Review, Volume XI, Number 236