Patterson Belknap

Privacy & Data Security Alert

July 2018

California's New Digital Privacy Law: Impact on Business Operations

California's landmark digital privacy law – enacted less than two weeks ago – is the most sweeping consumer data protection law in the United States. The California Consumer Privacy Act of 2018, or CCPA, will apply to more than 500,000 companies in the United States alone. It will also potentially affect global companies that do business in California and collect the personal information of the state's consumers.

The new law gives consumers unprecedented control over their personal information including the right to know what information companies are collecting about them, how it is used, and if it is sold to third parties. Consumers will also have the right to prohibit companies from sharing their personal data.

The bill was pushed through the state's legislature and signed by the governor hours before a deadline to remove from the November ballot an initiative that contained even tougher data security requirements. While the law is far from clear in many respects, the looming question is whether its core consumer protections will serve as a blueprint for other states in passing similar legislation.

The new requirements created by CCPA will drive dramatic changes in how businesses handle the personal information of California's consumers – requiring covered companies to overhaul their databases and tracking technologies. New compliance regimes will also be needed to monitor consumer requests and demonstrate that organizations are following the new rules.

Although the law does not go into effect until January 2020, industry organizations are already digging in and demanding changes to CCPA, with some critics calling the law "unworkable." But unless the California legislature is convinced to amend the statute, companies will need to start preparing now to ensure their compliance. In this Alert, we outline the key features of CCPA.

What new rights are created by the law? In broad terms, the new rights created by CCPA fall into four broad categories:

- ***Right to Know*.** Consumers may request disclosure of the categories and details about the specific information collected about them, their sources, purpose of collection, and what information is shared with third parties.
- ***Right of Deletion*.** Consumers may request that a business delete any personal information it has collected about them, subject to several exceptions.
- ***Right to Opt Out or Opt In*.** Consumers may opt out of any sale of their information to third parties.
- ***Right of Equal Service*.** Covered businesses are prohibited from discriminating against consumers exercising any of their rights under CCPA, including through pricing and quality of goods or services, unless different treatment is "reasonably related to the value provided to the consumer by the consumer's data." Businesses, however, are free to offer reasonable financial incentives to consumers related to the collection, sale, or deletion of their personal information.

What companies are affected? A covered "business" is any for-profit entity that "does business in the state of California;" has at least $25 million in annual revenues; holds the personal data of 50,000 people, households, or devices; or that receives at least half of its revenue in the sale of personal data. Practically speaking, this far-reaching definition will cast a wide net, sweeping up small, yet profitable, businesses that do business in California, wherever located. The law contains a series of exemptions – such as healthcare data covered by the Health Insurance Portability and Accountability Act, consumer report data governed by the Fair Credit Reporting Act, and personal information collected pursuant to the Gramm-Leach-Bliley Act. But the law, as written, applies to entities covered by these laws *if* they collect and process *other* information about California consumers.

What information is affected? CCPA's definition of personal information is uniquely broad, including any information that identifies or relates to, directly or indirectly, a particular consumer. Examples include:

- ***Unique Identifiers***. This category includes a consumer's name, alias, postal address, unique identifier, internet protocol address, electronic mail address, account name, Social Security number, driver's license number, and passport number.
- ***Protected Classifications***. This category covers protected classifications under California or federal law (such as race, gender, disability, and others protected by antidiscrimination laws).
- ***Commercial Information***. This category includes records of property; products or services provided, obtained, or considered; or other purchasing or consuming histories or tendencies.
- ***Internet Data***. This category includes internet or other electronic network activity information, including but not limited to browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement.

The statute also covers a laundry list of other types of personal information, including biometric data, geolocation data, and educational information.

"Personal information" does not include information that is publicly available or that is de-identified – i.e., information that cannot reasonably identify the consumer or device. Notably, the initiative has a narrow definition of what is "publicly available," limiting it to information that is "lawfully made available from federal, state or local government records or that is available to the general public."

What must businesses do to comply? Covered businesses will be required to make substantial changes in the way they handle consumer information and will need to create new compliance programs to document their efforts. By way of example, to comply with the "right to know" – consumers' right to know how their personal information is used – businesses will need to provide at least two methods by which consumers can get in touch with them, including a toll-free telephone number and website address. Other contact methods may include mailing address, email address, web portal, or any method approved by the Attorney General. Then, each business will need to create a compliance process to respond and to document its actions in accordance with the law.

Enforcement? Although the California Attorney General will have the right to enforce the law, there is also a private right of action for unauthorized access to a consumer's "nonencrypted or nonredacted personal information." If a company fails to address an alleged violation within 30 days, fines stack up quickly to the tune of $7,500 per violation.

We will continue to monitor developments related to CCPA and will post updates on our blog, https://www.pbwt.com/data-security-law-blog/, and send out updates as circumstances merit.

Please contact us with any questions.

This alert is for general informational purposes only and should not be construed as specific legal advice. If you would like more information about this alert, please contact one of the following attorneys or call your regular Patterson contact.

Craig A. Newman 212-336-2330 cnewman@pbwt.com

Alejandro H. Cruz 212-336-7613 acruz@pbwt.com

Maren J. Messing 212-336-7645 mmessing@pbwt.com

Kade N. Olsen 212-336-2493 kolsen@pbwt.com

Simone M. Silva-Arrindell 212-336-2165 ssilvaarrindell@pbwt.com