OCBJ.COM

ORANGE COUNTY BUSINESS JOURNAL

Vol. 40, No. 43 THE COMMUNITY OF BUSINESS™ October 22-28, 2018 • $1.50

PAYNE & FEARS
ATTORNEYS AT LAW

It's No Secret: California's New Consumer Privacy Law Goes Live in 2020 (Maybe)

Privacy activists cheered when, on June 28, 2018, Governor Brown signed into law the strictest consumer privacy law in the United States; the California Consumer Privacy Act of 2018 ("CCPA"). Effective January 1, 2020, the CCPA imposes a range of new requirements on businesses to ensure that consumers enjoy choice and transparency in the treatment of their personal information.

Who is Protected?
The CCPA protects the personal information of "consumers" – who are individuals defined as Californian "residents" in California's personal income tax regulations.

Who is Regulated?
The CCPA applies to for-profit businesses that (1) do business in California, (2) collect consumers' personal information (directly or through a third party), and (3) determine the purpose and means of processing that personal information (directly or jointly). And meet one of the following three thresholds: (1) have annual gross revenues in excess of $25 million; (2) annually buys, sells, receives for commercial purposes, or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices; or (3) derives 50 percent or more of its annual revenues from selling consumers' personal information. Entities that control or are controlled by a business that meets the criteria can also be subject to the CCPA if their commercial conduct takes place in California.

What Information is Regulated?
The CCPA has a significantly more expansive definition of "personal information" than prior privacy laws, and is not limited to personal information collected online. The expanded definition includes any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked with a particular consumer or household. This would include names, addresses, social security numbers, IP addresses, educational information, inferences drawn to create a profile about the consumer, consumer preferences, etc.

Excluded from the CCPA's definition of "personal information" is data which (1) is publicly available; (2) cannot reasonably identify, relate to, or describe a particular consumer (provided safeguards are taken to protect against re-identification); and (3) relates to a group or category of consumers from which individual identities have been removed (provided it is not linked or reasonably linkable to a particular consumer or household). Information is not considered to be publicly available if it is used for a purpose other than the purpose for which it is maintained and made available in government records, or for which it is publicly maintained.

Given the expansive scope of the CCPA, businesses may find that they are inadvertently collecting "personal information" under the CCPA. For example, an Internet blogger with more than 50,000 subscribers, who shares its subscribers' information with advertisers, likely falls within the CCPA.

What is Required?
The CCPA empowers California residents to: (1) know what personal information is being collected; (2) know whether their personal information is sold or otherwise disclosed, and to whom; (3) reject the sale of their personal information; (4) access their personal information and request deletion; and (5) receive equal service and price from the business, even if the resident exercises its privacy rights under the CCPA.

In addition, the CCPA requires businesses to provide certain notices and disclosures to its consumers. In particular, businesses must inform its consumers about: (1) the categories of personal information the business collects and the purposes for which the information will be used; (2) the consumers' right to request that the business delete their personal information; and (3) the consumers' right to opt out from the sale of personal information. Consumers also have a right to request and receive the following information, including: (1) the categories and specific personal information collected by the business; (2) the categories of sources from which the personal information is collected; (3) the purpose for which the personal information is collected; (4) the categories of third parties with whom the personal information is shared; and (5) the categories of personal information that the business sold or disclosed for a business purpose.

The Consequences for Violations
The CCPA has two substantial enforcement mechanisms. First, the Attorney General may penalize violators with civil penalties if violations are not cured within 30 days, ranging $2,500 to $7,500 *per violation.*

In addition, the CCPA creates a private right of action which allows California residents to recover between $100 to $750 *per incident* (or actual damages, whichever is greater) if their personal information is compromised as a result of the business' failure to implement and maintain reasonable security procedures. The amount of statutory damages will be determined by a court, which will evaluate various factors such as the nature, seriousness, volume, and persistence of the violations.

The CCPA requires consumers to provide 30 days' notice to the business of the alleged violations before filing suit. If the violation is cured and the business provides the consumer a written statement that the violations have been cured and that no further violations shall occur, the consumer cannot proceed with the lawsuit. However, if the business continues with its alleged violations, the consumer can sue for the original and any new CCPA violations, including a breach of the written statement. This 30-day notice is not required if the consumer suffered actual pecuniary damages as a result of the business' failure to implement and maintain reasonable security procedures.

What the Future Holds
Businesses should understand that the CCPA was passed as part of a deal brokered between Sacramento and proponents of a competing ballot initiative which would have imposed even stricter data privacy rules on companies doing business in California. These privacy advocates imposed a deadline by which Governor Brown had to sign the CCPA, but agreed to remove their ballot initiative once it was signed into law. While the compromise averted a costly fight over the proposed ballot initiative, it also produced a hastily-drafted law that leaves a multitude of unanswered questions for businesses. For example, it is unclear if the $25 million annual gross revenues threshold is limited to those revenues generated in California, or if it encompasses annual gross revenues worldwide. Given the definition of "consumers" in the CCPA, another open question is whether the law applies to covered entities that process even a single California resident's personal information, no matter where that entity is located. It is also unclear how personal information should be deleted in response to a consumer's request or how such deletion should be tested.

The confusion is not limited to businesses. In fact, the California Attorney General has questioned its own ability to meet the operational obligations of the new law. And privacy advocates have criticized the exclusion of state and local governments from the requirements of the CCPA. Finally, there is a growing movement in Washington to craft federal privacy laws that would preempt the CCPA, and empower the Federal Trade Commission with nationwide enforcement.

With so many open questions and competing interests, California's Legislature is certain to consider additional changes when it reconvenes for the 2019 session. Businesses should monitor future amendments to the law and the adoption of corresponding regulations by the Attorney General, which will likely affect the CCPA's impact on day-to-day business.

Robert T. Matsuishi is an attorney in the Irvine office of Payne & Fears LLP. He has extensive litigation and counseling expertise in complex business and labor and employment matters, including trade secret misappropriation, non-competition agreements, employee and consumer privacy, breach of contract, wrongful termination, discrimination, harassment, and retaliation. He can be reached at rtm@paynefears.com.

Nathan A. Cazier ("Nate") is a partner in the Irvine office of Payne & Fears LLP, with more than a decade of insurance litigation experience representing and advising policyholders regarding all types of insurance. Nate also counsels clients regarding cybersecurity and data privacy issues, with an emphasis on the emerging market of cyber insurance, and represents corporations of all sizes in their commercial and employment disputes. Nate can be reached at nac@paynefears.com.