LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
THURSDAY, SEPTEMBER 19, 2019

PERSPECTIVE

State Legislature amends key privacy law to take effect in January

By Grant Davis-Denny and Nefi Acosta

The California Consumer Privacy Act, which was enacted in June 2018 and is set to take effect on Jan. 1, 2020, is the country's most sweeping privacy law and imposes an assortment of new operational requirements on many companies that do business in California. On Sept. 13, the California Legislature passed six bills amending the CCPA. Although these amendments still require the governor's signature, we now have a better sense of what the CCPA will require when it takes effect in just over three months.

The CCPA's Key Requirements Still Will Take Effect on Jan. 1, 2020: The most important takeaway from the amendment process is that the CCPA's main provisions are still intact. The statute continues to cover a vast array of personal information — basically any electronic or paper data reasonably linkable to a particular individual or household that is not available in government records — and regulates a large number of for-profit businesses — including businesses based inside or outside the state that have at least $25 million in revenue or data on at least 50,000 Californians and that do business in California. The CCPA's key mandates also remain fundamentally unchanged. Covered companies must provide consumers with notice of data collection practices at or before the point of collection; they must respond expeditiously to consumer requests for access to or deletion of their data; and they must comply with consumers' decisions to opt out of having their data sold. A host of other operational changes — such as revisions to website privacy policies, new links on company websites for opting out of data sales, and additional training requirements for employees who handle data subject access requests — also remain in place. In short, for businesses that collect significant volumes of consumer data and that are covered by the CCPA, implementing an effective CCPA compliance program is still a must, even after the recent amendments.

Although these amendments still require the governor's signature, we now have a better sense of what the CCPA will require when it takes effect in just over three months.

The One-Year Exemption for Employee Data: The amendments' most significant beneficiaries are companies that possess large volumes of data about California-based employees, but little or no data on individual customers. The amendments temporarily exempt data about such employees — as well as job applicants, contractors, owners, directors, officers, and medical staff members — from the CCPA's scope. This, however, is but a one-year reprieve; the exemption will expire on Jan. 1, 2021. Moreover, businesses are still required to give employees notice at or before the point of collection of the categories of data being collected and the purposes for which the data will be used. And employers who suffer a data breach involving employees' sensitive personal information (for example, stolen names and social security numbers) can be subject to an employee lawsuit for statutory damages of up to $750 per affected individual. The amendments also include a one-year exemption for certain communications and transactions that occur as part of business-to-business transactions, though this data is still subject to the CCPA's sales-opt-out, non-discrimination, and statutory damages provisions.

Data Brokers Registration: A notable addition to the CCPA is a requirement that data brokers register with the California Attorney General. The amendment defines a "data broker" as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." The data- broker registration duty potentially could apply to a large number of businesses that receive consumer information through business partners because the CCPA broadly defines a "sale" to mean the transfer of data in exchange for any "valuable consideration"—not just money. But entities covered by the Fair Credit Reporting Act (FCRA), Gramm- Leach-Bliley Act, and the Insurance Information and Privacy Protection Act are expressly excluded from the definition of "data brokers" and are not required to register. On a yearly basis, data brokers must (1) pay a registration fee yet to be determined by the Attorney General and (2) register their name, physical, email, and website addresses with the Attorney General. In turn, the Attorney General must make this information publicly accessible online. Data brokers that fail to register are subject to a $100 fine per day of noncompliance, in addition to other civil penalties.

Covered Data: An amendment has modestly narrowed the CCPA's definition of "personal information" by requiring that such data be not merely linkable to a particular individual, but that it be "reasonably" linkable. Additionally, the amendments make clear that aggregated or de-identified data are not classified as "per-

sonal information" and thus do not fall under the CCPA's requirements. Finally, the amendments clarify that "publicly available" data — a category of data excluded from the definition of "personal information" — is information that is lawfully available in government records.

Industry-Specific Exemptions: The amendments exempt certain credit- related information that is used by a credit reporting agency, a provider of credit information, or a user of such information if the data is subject to and is used consistent with the federal FCRA; the CCPA's private right of action for statutory damages, however, could still apply to such data if it is stolen in a breach. Another amendment exempts vehicle or owner information from the CCPA's opt-out right if the information is used for warranty- or recall-related repairs and the information is not sold, shared, or used for any other purpose.

Data Subject Access Request Methods: As originally written, businesses were required to provide consumers with at least two methods for exercising their CCPA data access, deletion, and sales-opt-out rights, including a toll-free telephone number. One of the passed amendments creates an exemption for businesses operating exclusively online that have a direct relationship with consumers from whom they collect personal data. Such entities may provide consumers with only an email address in lieu of providing a toll-free telephone number and a second method for exercising data subject access request rights. ■

Grant Davis-Denny *is a partner at Munger, Tolles & Olson LLP. He regularly advise clients on proactive data security and privacy issues. Mr. Davis-Denny may be reached at Grant.Davis-Denny@mto.com.*

Nefi Acosta *is an associate at Munger, Tolles & Olson LLP. He regularly advise clients on proactive data security and privacy issues. Mr. Acosta may be reached at Nefi.Acosta@mto.com.*