LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
WEDNESDAY, OCTOBER 7, 2020

PERSPECTIVE

2020 brings another set of new California privacy laws

By Grant Davis-Denny

With the 2018 passage of the California Consumer Privacy Act, California established itself as the undisputed leader among the states in enacting aggressive privacy laws. California's privacy landscape has continued to evolve since 2018, and 2020 is turning out to be no exception. In the final days of the 2020 session, the California Legislature enacted and the governor signed three new privacy bills. One is of significant interest to businesses with California employees or contractors and for businesses that interact with California individuals as part of a business-to-business relationship. The other two bills are primarily of interest to companies in specific sectors: (1) health care and related research; and (2) direct-to-consumer genetic testing. This article analyzes these three bills and their relationship to the previously enacted CCPA and the California Privacy Rights Act, an initiative that is on the ballot this November.

Extension of the CCPA's Employee and B2B Exemption

As originally enacted, the CCPA applied to data about any California resident, and was not limited to end consumers, as that term is commonly understood. In 2019, as the CCPA's effective date of Jan. 1, 2020, approached, the California Legislature exempted certain data about employees, job applicants, contractors, and information collected as part of B2B interactions from most, though not all, of the CCPA's provisions. But the Legislature opted to sunset these exemptions on Jan. 1, 2021.

In the final days of the 2020 session, the California Legislature enacted and the governor signed three new privacy bills. One is of significant interest to businesses with California employees or contractors and for businesses that interact with California individuals as part of a business-to-business relationship.

One of the newly enacted laws, Assembly Bill 1281, extends these exemptions for one additional year to Jan. 1, 2022, unless voters pass the CPRA in November 2020. If the CPRA passes, AB 1281 will not take effect. But the CPRA contains its own extension of the employee and B2B exemptions through Jan. 1, 2023 (one year longer than AB 1281's extension). The upshot for businesses is that the existing employee and B2B exemptions will not expire on Jan. 1, 2021, will continue until at least Jan. 1, 2022, and likely will remain in place until Jan. 1, 2023. And before the exemption expires, the California Legislature or voters could enact yet another privacy law, this time specifically targeted at employee and B2B data.

Aside from extending the employee and B2B exemptions, AB 1281 does not modify the exemptions' substance. They continue to only partially exclude employee and B2B data from CCPA provisions. The CCPA's requirement that businesses provide notice at or before the point of collection of what data is being collected and how it will be used thus still applies to both categories of data. Similarly, the CCPA's statutory damages provision for certain data breaches also will continue to apply to employee and B2B data. Additionally, the CCPA still requires businesses that sell B2B data to allow California residents to opt out of information sales and prohibits businesses from discriminating against California residents who exercise their CCPA rights related to B2B data.

Refinement of the CCPA's Exemption for Health Data

When the Legislature originally passed the CCPA, it included an exemption for data regulated by HIPAA or California's Confidentiality of Medical Information Act, an exemption for providers of health care and HIPAA-covered entities, and a narrowly defined exemption for data collected as part of certain clinical trials.

The second key California privacy law of 2020, AB 713, expands these exemptions. For example, AB 713 exempts from the CCPA certified patient information that is deidentified in accordance with HIPAA's requirements for deidentifying protected health information. But if this information is ever reidentified, it again becomes subject to the CCPA. Additionally, businesses that sell or disclose deidentified information must include in their privacy notice the fact that they do so and the deidentification methodology that they use. Deidentified information that is sold after Jan. 1, 2021 must be done pursuant to a contract that restricts reidentification.

AB 713 also expands the current exemption for HIPAA covered entities to exclude "business associates" of a HIPAA covered entity "to the extent the business associate maintains, uses, and discloses patient information in the same manner as" HIPAA-protected health information or CMIA-protected medical information.

Finally, AB 713 enlarges the CCPA exemption for clinical trials by excluding other forms of "research," as that

term is defined in HIPAA regulations. "Research" means any "systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." This is a significantly broader set of research activities than were exempted by the CCPA's prior clinical-trial exemption. Moreover, while the CCPA previously only exempted data that was collected as part of a clinical trial, the AB 713 exemption also will apply to data used or disclosed, as well as collected, as part of research activities. To qualify for this exemption, AB 713 adds a requirement that a business conduct the research in accordance with HIPAA's security, privacy, ethics, and confidentiality requirements.

Genetic Testing

Although the CCPA's privacy protections for personal data typically would cover genetic testing data related to a California resident, the California Legislature determined that more aggressive regulation is needed for direct-to-consumer genetic testing data. Senate Bill 980, the Genetic Information Privacy Act, creates a series of new requirements for direct-to-consumer genetic testing businesses and their business partners.

SB 980, for example, requires enhanced privacy notices from genetic testing companies. On top of disclosing collection, use and disclosure practices, genetic testing companies' privacy notices must include "complete information" about their consent, maintenance, retention, and deletion practices. Consumers also must receive information about how to exercise their complaint rights under SB 980, and businesses must inform California residents that their data may be disclosed to third parties for research purposes.

The new law also subjects direct- to-consumer genetic testing companies to heightened consent requirements. In particular, the consent must be express and separately obtained for use, post-testing storage, transfers to third parties, and marketing of genetic testing data, and details such as the name of the third party must be shared in connection with obtaining the consent. These companies must adopt methods for consumers to revoke their consent and then honor these revocation requests as soon as possible and no later than 30 days after the request is made. SB 980 also restricts genetic testing companies' ability to share data with those responsible for making employment decisions or decisions about health, life, long-term care or disability insurance.

SB 980 authorizes civil penalties of up to $1,000 per negligent violation and up to $10,000 per willful violation. Penalties must be paid to the individuals whose genetic data was involved in the violation. The statute authorizes civil actions brought not only by the Attorney General and by local district, county, and city attorneys, but by any person who has had an injury in fact and who has lost money or property as a result of a violation of SB 980.

2020 (Unfortunately) Is Not Over Yet

While the legislative session has concluded, polling indicates voters likely will pass next month the CPRA, 2020's most sweeping change to California privacy laws. A full discussion of the CPRA, which substantially amends the CCPA, is beyond this article's scope. But if the CPRA passes, a new enforcement agency called the California Privacy Protection Agency will be created and businesses that handle California consumer data will be required in certain circumstances to respond to consumers' requests to correct inaccurate personal information, consumers' requests to opt out of the sharing of personal information, and consumers' request to limit use of sensitive personal information. If enacted, these new requirements would take effect in 2023, with implementing regulations to be adopted by July 1, 2022. In short, businesses that invested substantial resources in designing and implementing CCPA compliance programs likely will have to continue to evolve their programs over the next two years in preparation for the CPRA taking effect. ■

Grant Davis-Denny *is a litigation partner at Munger, Tolles & Olson and focuses his practice on complex litigation and data privacy and data security matters.*