DORSEY
DORSEY+WHITNEY LLP

Three More California Privacy Bills Become Law: CPPA Rulemaking Responsibility, Genetic Data Breaches, and New Genetic Information Privacy Act

by Melonie S. Jordan

Californians voted to enact the California Privacy Rights Act ("CPRA") almost one year ago. Last week, Governor Gavin Newsom signed three new privacy bills into law. Through the bills, the California Legislature amended the CPRA by clarifying the timing for CPRA rulemaking, extended California's data breach notification law to include genetic data, and enacted a new law that further protects genetic data. Through these new laws, California has expanded protections for its residents' most enduring personal information.

The California Consumer Privacy Act ("CCPA") took effect January 1, 2020. Later that same year, California voters approved the CPRA in the November 3, 2020 statewide general election. By approving the CPRA, California voters substantially amended and expanded the CCPA and established the California Privacy Protection Agency ("CPPA") which will administratively enforce the CCPA as amended by the CPRA. Last week's new laws include another wave of changes with which organizations must comply.

The first bill signed by Governor Newsom, Assembly Bill 694 ("AB 694") includes clarifications of CPRA provisions on rulemaking responsibility timing.[1] Currently, under Civil Code Section 1798.199.40(b), the CPPA assumes rulemaking responsibility the *earlier* of July 1, 2021, or within six months of the CPPA notifying the Attorney General that it is prepared to assume responsibility. However, under Civil Code Section 1798.185(d), the CPPA assumes rulemaking responsibility on the *later* of these two dates. In AB 694, the Legislature synced these two sections by amending Section 1798.199.40(b), to clarify that the CPPA assumes rulemaking responsibility on the *later* of the two dates.

Through the second bill signed by Governor Newsom, Assembly Bill 825 ("AB 825"), the California Legislature expanded the definition of "personal information" in California's data breach law. Civil Code Section 1798.82, requires covered businesses to notify California residents of a breach in the security of the residents' unencrypted personal information. Similarly, Civil Code Section 1798.81.5 requires businesses that own,

Related People

- Melonie S. Jordan

Related Capabilities

- Privacy & Social Media
- California Consumer Privacy Act (CCPA)

license, or maintain personal information to provide reasonable security for that information. Under Civil Code Section 1798.150, California residents whose non-encrypted or non-redacted personal information is breached may sue for damages.

"Personal information" now includes "genetic data," defined as:

[A]ny data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material. Genetic material includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom.

Cal. Civil Code § 1798.82(h)(1)(H). This change "ensures that residents are … informed when their most sensitive and immutable data, their genetic data, is subject to a breach."[2]

Through the third bill signed by Governor Newsom, Senate Bill 41 ("SB 41"), the Legislature established the Genetic Information Privacy Act ("GIPA"), which governs direct-to-consumer ("DTC") genetic testing companies and their vendors. Under the GIPA, DTC genetic testing companies must provide a consumer with clear and complete information regarding the company's collection, use, maintenance, and disclosure of genetic data. These companies must obtain a California consumer's express consent for collection, use, or disclosure of the consumer's genetic data, including obtaining separate consents in a number of different scenarios including storage, transfer, and marketing use. Should a California consumer revoke consent, DTC companies must honor the revocation and destroy the consumer's biological sample within 30 days. Companies must ensure reasonable security of genetic data. Under the GIPA, companies may face civil penalties for violations. Actions for relief will be prosecuted by the Attorney General, district attorney, county counsel, city attorney, or city prosecutor in the name of the people of the State of California. By enacting the GIPA, the California Legislature sought to "provide adequate guidelines for what can be done with genetic data collected by companies outside of the protective ambit of state and federal health privacy laws."[3] The GIPA is effective on January 1, 2022.

In light of the expansion of protection of genetic data, DTC genetic testing companies should update their policies and procedures to address the safekeeping of genetic data. DTC genetic testing companies should also implement policies and procedures to facilitate destroying consumers' biological samples in a timely manner, upon request.

As the effective dates of the CPRA and the GIPA near, your Dorsey CCPA Team can effectively guide your organization through developing and implementing proactive California-compliant programs. Be sure to contact your Dorsey attorney for assistance in navigating California's privacy landscape.

[1] See the Assembly Floor's analysis of AB 694.

[2] See the Senate Floor's analysis of AB 825.

[3] See the Senate Floor's analysis of SB 41.