EPSTEIN BECKER GREEN

Health Law Advisor

Thought Leaders on Laws and Regulations Affecting Health Care and Life Sciences

Follow the Leader: California Paves the Way for Other States to Strengthen Privacy Protections

By Daniel Kim & Alaap Shah on March 7, 2019

Consumer privacy protection continues to be top of mind for regulators given a climate where technology companies face scrutiny for lax data governance and poor data stewardship. Less than a year ago, California passed the **California Consumer Privacy Act (CCPA) of 2018**, to strengthen its privacy laws. In many regards, the CCPA served as a watershed moment in privacy due to its breadth and similarities to the E.U. sweeping **General Data Protection Regulation (GDPR)** law.

Yet, California continues to push the envelope further. Recently, California State Senator Jackson and Attorney General (AG) Becerra introduced a new bill (**SB561**) that will expand the consumer's right to bring private lawsuits for violations of the CCPA. If passed, SB561 will: (1) provide for a private right of action for all CCPA violations—not just those stemming from a data breach; (2) eliminate the 30-day period for businesses to cure after receiving notice of an alleged violation; and (3) allow the AG to publish guidance materials for businesses instead of allowing businesses' the option to seek specific opinions of the AG. Currently, the CCPA allows the AG office to bring action against business, in most instances, only allowing consumers to bring private action in instances of data breach resulting from a business's failure to implement reasonable security measures. If SB561 is passed, the CCPA will materially expose businesses to private actions for damages applicable to other violations under the CCPA, including failure to provide consumers with proper notifications required under the CCPA.

These developments are just the tip of the iceberg. Emboldened by California's example, many other states are following suit. As such, businesses that implement an effective CCPA compliance program will likely position them to satisfy potential compliance obligations in other states moving forward. For example, Colorado recently passed as sweeping law to protect patient privacy (**HB18-1128**), which went into effect September 1, 2018. Colorado now requires covered entities (e.g., business entities that maintain, own, or licenses personal identifying information (PII) in the course of their business) to implement, and ensure that third-party service providers implement, reasonable security procedures and practices. Additionally, the law requires covered entities to develop written policies and procedures concerning the destruction of paper and electronic documents that contain PII. Further, the law authorizes the AG to bring criminal prosecution against covered entities that violate the new rules.

Other states including **Hawaii**, **Maryland**, **Massachusetts**, **New Mexico**, **New York**, **North Dakota**, **Rhode Island**, and **Washington** are also using the CCPA and the **GDPR** as templates to perform similar overhaul of their privacy laws. As a result of this state law trend, businesses should closely monitor the legislative progress of these state bills. Further, if businesses have not yet started shoring up their privacy and data security practices and programs, they had better do so in short order. It is likely that many of these state laws, if passed, will carry stiff penalties for noncompliance and may subject businesses to class actions.

In addition to these piecemeal state law efforts to strengthen privacy, the U.S. Chamber of Commerce is currently exploring whether a **Federal consumer privacy protection law** should be enacted. It appears that the privacy tidal wave starting on California's west coast is making its way eastward . . . .

Daniel Kim

Alaap B. Shah

Health Law Advisor

EPSTEIN BECKER GREEN