Mitigating your Business Risk

Compliance with Data Privacy Laws

BY WILLIAM R. DENNY

BUSINESSES LARGE AND SMALL are facing unprecedented liability and reputational harm due to cyber-attacks and data breaches. Financial institutions, private businesses, public agencies, and now the City of Baltimore have had their networks frozen by ransomware. In response to this, and to sweeping new data privacy laws in Europe, states and the federal government have pushed for new laws regulating data privacy.

California's sweeping new data privacy law, passed in 2018, represents a seismic shift in how businesses in the U.S. must deal with personal information. The California Consumer Privacy Act ("CCPA") goes into effect on January 1, 2020, forcing businesses to take a dramatic leap from the traditional approach toward privacy in the U.S., that of notice, to an approach that affords significant rights and controls to individual consumers. Businesses throughout the U.S., not just in California, will need to re-design their data security and privacy practices to avoid potentially significant liability.

What Is the CCPA?

The CCPA grants consumers the right to know what information companies are collecting about them, why they are collecting that data and with whom they are sharing it. It gives consumers the right to tell companies to delete their information as well as not to share their data, and it protects consumers from discrimination. Businesses have extensive reporting and record-keeping obligations under the CCPA and consumers and the California Attorney General have broad remedies, including a private right of action in the event of a data breach that provides for statutory damages of up to $750 per individual per incident.

Who Must Comply With the CCPA?

The CCPA applies to all for-profit businesses that collect personal information of California residents and satisfy one of the following thresholds: (1) annual gross revenues in excess of $25 million, (2) annually receives or shares the personal information of 50,000 or more consumers, households or devices, or (3) derives 50% or more of its annual revenues from selling consumers' personal information. If a company, for example, has a commercial website that attracts just 137 unique visitors per day, it would be subject to the CCPA, even if only a tiny subset of its customers were residents of California. The law also applies to service providers of such businesses. In all, it is estimated that over 500,000 U.S. businesses will be subject to the new law.

What Information Falls under the CCPA?

The CCPA addresses the "personal information" of a "consumer." "Personal information" is incredibly broad, and includes any information that is capable

of being associated with a particular consumer or household. This would include a person's name, contact information, email address, financial and health information, but also a person's biometric and location data, purchasing history, internet browsing history and even IP address. While there are exclusions for health data covered by HIPAA and financial data covered by the Gramm-Leach-Bliley Act ("GLBA"), carve-outs to the exceptions bring health and financial institutions squarely back within the CCPA. For one thing, because the definition of "personal information" is so much broader than the information covered by HIPAA or GLBA, it is likely that banks and health care providers collect a significant amount of data that is subject to CCPA compliance rules. Moreover, individuals are granted a private right of action against banks if their data, including financial data regulated by the GLBA, is breached due to failure to implement reasonable security. This subjects banks to class-action lawsuits and potentially staggering statutory damages without the requirement that individuals prove actual damages.

The definition of "consumer" is also extremely broad, meaning "a natural person who is a California resident." It is not limited to customers of a business, and therefore includes the business's employees and the employees and customers of business partners and service providers. It also includes California residents who temporarily live outside of California, increasing the compliance challenges to businesses.

First Steps toward Compliance

In preparation for the CCPA becoming effective, businesses should consider the following steps in consultation with a legal advisor:

Assess whether you are subject to the CCPA. If you do any business in California and you have annual gross revenues exceeding $25 million, or if you collect information from at least 137 unique visitors per day or derive half of your annual revenue from selling consumers' personal information, then the law likely applies to you.

Conduct a data inventory. To comply with the CCPA, you need to know your data. You must know what personal information you collect, where it is collected and stored, and whether, to whom and for what purpose it is shared or sold.

Begin to preserve data. The CCPA has a 12-month look-back period, so businesses will need to report details of their data collection, handling and sharing going back to January 1, 2019.

Update your privacy policy. The CCPA includes many new elements and consumer rights that are required to be described specifically in online privacy notices.

Implement a process to respond to data access requests. Once the CCPA takes effect, California residents will have the right to request information about the categories of personal information collected about them going back 12 months, and businesses must have a way to verify these requests and respond to them within 45 days.

Update agreements with service providers. Businesses should ensure, by written agreement, that service providers are complying with the data sharing and usage restrictions at the core of the CCPA. Such agreements will allow businesses to transfer data to service providers without it being considered a "sale" subject to the consumer's opt-out right.

Assess security measures. The CCPA grants a private right of action to consumers affected by a data breach, where businesses have failed to take "reasonable" security measures to protect their data. The California attorney general has provided guidance that to have reasonable security, businesses should at least have implemented the 20 controls outlined by the Center for Internet Security.

Key Takeaway

Understanding the CCPA's requirements and implementing robust policies and procedures to comply with them is essential. Not only will the CCPA be a major part of the regulatory landscape, but lawmakers in numerous other states have introduced "copycat" laws modeled on the CCPA, including Connecticut, Hawaii, Maryland, Massachusetts, Nevada, New Jersey, New Mexico, New York, North Dakota, Texas and Washington. Building a strong approach to data privacy in line with the CCPA's requirements will position a business for success when other laws at the state or federal law are enacted. ■

William Denny is a Partner and Head of Cybersecurity, Data Privacy and Information Governance Practice Group at Potter Anderson & Corroon LLP.