Is Your Business Ready for the California Consumer Privacy Act?

By David J. Oberly

The most significant piece of privacy legislation in the United States to date — the California Consumer Privacy Act of 2018 (CCPA) — is set to go in effect in just a few months, on January 1, 2020. When that time comes, the CCPA will impose a broad set of onerous requirements on companies relating to how they collect, use, disclose and sell consumer personal data.

Although the name of the law suggests that the CCPA applies only to companies located in California, the reach of the CCPA will actually extend nationwide. Specifically, any business that collects the personal data of California residents and meets any one of three thresholds will be required to comply with CCPA mandates.

This means that many Ohio businesses (including law firms)—even if they have no physical presence in California — will be required to comply with the CCPA once it goes into effect at the start of next year.

Determining CCPA Applicability

One of the more significant aspects of the CCPA pertains to the broad scope of business entities to which the law applies. For Ohio companies, then, the first matter to address is determining whether the CCPA applies to their operations.

The CCPA applies to any business that handles the personal data of California residents and meets any one of three thresholds:

1. Has annual gross revenue in excess of $25 million;
2. Collects, buys or sells the information of 50,000 or more consumers, households or devices; or
3. Derives 50 percent or more of its revenue from the sale of consumers' personal information.

Significantly, a physical presence in California is *not* a requirement to fall under the scope of the law. Rather, any company that does business in California — even if the entity is not located within the state's borders — must comply with the mandates of the CCPA if it handles California consumers' personal information and meets any of the three thresholds.

Compliance with CCPA

If an Ohio business determines that it falls under the scope of the CCPA, that entity will be required to comply with a range of different privacy-related mandates regarding how it utilizes consumers' personal data in the course of its business operations. Consequently, the business will have to devote a significant amount of time, energy and resources to make the necessary

updates and modifications to its operations to get in compliance by the start of next year.

The first operational response for compliance with the CCPA is to conduct a data mapping and inventory analysis of all personal data that's handled by the company. To accomplish this task, businesses will need to map and inventory every piece of personal information that is collected, used and sold by the company, as well as all of the company's data-processing practices. In doing so, the company will need to analyze all aspects of its business operations, and all points where the company collects, handles or transmits personal data from any source and in any format. From there, the company should maintain its organization-wide data inventory (comprising *all* of the company's data) in order to ensure that data is well-prepared to satisfy consumer requests. Ideally, a company's mapping and inventory practices should enable the company to identify data location information as it relates to specific individuals; doing so will enable the company to respond to the myriad different consumer requests that are permissible under California's privacy law.

After completing the data mapping and inventory exercise, the next step is to develop systems and procedures to ensure adherence with the range of broad rights that have been afforded to consumers under the new law. Specifically, businesses will have to comply with the following rights:

- **Right to Know:** Consumers must be able to learn — through a general privacy policy and with more details upon request — what personal information a business has collected about them, where the information originated, the use of the information, and whether and to whom the information is being disclosed or sold.
- **Right to Access:** Consumers can request that businesses provide them with a copy of all personal information collected by the entity on the consumer; the business must provide this information to the consumer free of charge.
- **Right to Opt-Out:** Businesses must allow consumers to "opt-out" and stop a business from selling their personal information to third parties, with the term "sale" defined very broadly to include any sharing of personal information in exchange for something of value.
- **Right to Deletion:** Consumers maintain the right to request that businesses delete their personal information and data, subject to several exceptions.
- **Right to Equal Service & Pricing:** Consumers maintain the right to receive equal service and pricing from businesses, even if the consumer chooses to exercise his or her privacy rights under the CCPA.

Vendors, Cyber Insurance and Other Considerations

Businesses will also have to provide the mandated privacy disclosures and notices that are required by the CCPA. Here, companies will need to update