

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

CINCINNATI'S CREDIT CARD PROCESSING PROVIDER

Supporting The Cincinnati Legal Community



SECURE ONLINE
PAYMENT
PROCESSING



LOWERED FEES
FOR
CBA MEMBERS



NEXT DAY FUNDING
ON ALL
TRANSACTIONS



MIDWEST
PAYMENT PROCESSING

MIDWESTPAY.COM 513.274.2600

SEND A MONTHLY PROCESSING STATEMENT TO SALES@MIDWESTPAY.COM FOR AN ANALYSIS

their privacy policies with the information that's required to be affirmatively disclosed to consumers pertaining to the entity's data practices and consumers' rights under the CCPA — including a toll-free number and a website for consumers to submit requests, as well as a link on the company's website (titled "Do Not Sell My Personal Information") to facilitate the opt-out process. Companies must also develop the operational capabilities to provide information to consumers upon request in the event a consumer seeks information regarding the data collected and sold by the company, including the specific pieces of information that the business has collected concerning that consumer.

Additionally, businesses will need to ensure that they implement the necessary data security measures to comply with the CCPA's "reasonable" security requirement. Although the CCPA doesn't impose any express, direct data security requirements on businesses, it does require that covered entities put in place "reasonable security procedures and practices" to protect personal information from being improperly accessed or acquired by unauthorized third parties.

If consumer data is impacted by a data breach event and the business is found to have violated its duty to implement reasonable security measures, consumers are entitled to pursue class-action litigation under the CCPA's private right of action provision. Consumers can recover between \$100 and \$750 in statutory damages *per incident* if their data is compromised by a data breach. Although this damages figure may seem small, businesses must keep in mind that a class of just 10,000 consumers under the CCPA would subject a company to \$7.5 million in potential exposure.

Businesses will also need to update their contracts with vendors — aka "service providers" — to take into consideration the new issues raised by the CCPA. To maintain the ability to share information with vendors that perform services for them, businesses must enter into written agreements containing several mandatory provisions limiting the actions that vendors can take with respect to the company's personal information. In addition to updating contracts, businesses

will also need to ensure that its vendors continue to adhere to CCPA requirements over time through ongoing monitoring. Vendors should be regularly reviewed and evaluated, such as by using data security assessment questionnaires; vendors handling more sensitive data should be subject to a more exacting review (such as through third-party CCPA compliance audits). In doing so, all audits should be conducted through legal counsel to ensure that audits are shielded by attorney-client privilege.

Ohio businesses should also examine their cyber insurance coverage to ensure that their policies extend to cover the full range of CCPA-related liabilities. While privacy liability is ordinarily a staple in most cyber insurance policies, this coverage is often triggered only in the event of a data breach. Under the CCPA, though, a wide range of privacy violations can still take place outside of a data breach context; hence, many companies may find that their current cyber coverage does not adequately shield them against the CCPA's broad statutory liabilities.

To avoid any gaps in coverage, covered businesses must ensure that their policies provide coverage for acts or omissions stemming from the collection, use, disclosure and storage of "personal information" (as that term is used in the CCPA). In addition, cyber policies should also afford coverage for legal fees associated with regulatory investigations, regulatory fines, data breach response costs and liabilities stemming from class-action litigation.

A Game-Changing Scope

Ultimately, the CCPA will undoubtedly be a game-changer as it relates to the landscape of privacy law, in California and across the United States. The CCPA applies not just to companies with operations in that state, but all entities — regardless of where they are located — that handle the personal data of California residents. And since 20 percent of the nation's consumers reside in the Golden State, it's likely that many Ohio businesses, even those without any physical presence in California, will fall under the scope of the CCPA.

Because the law is set to go into effect in less than four months, Ohio companies must take action now to determine if the CCPA applies to them and, if so, immediately begin the process to achieve compliance by the January 1, 2020 effective date. Due to the law's breadth and complexity, it's recommended that companies utilize the services of outside legal counsel well-versed and experienced in privacy law (and the CCPA in particular) to guide the organization in the necessary action steps to comply with the law's broad range of mandates.

Oberly is an Associate Attorney in the Cincinnati office of Blank Rome LLP, and is a member of the firm's Data Privacy/Cybersecurity practice group. He can be reached at doberly@blankrome.com. Twitter: @DavidJOberly.

Can't Settle Your Case And Don't Want To Take It To Trial?

TRIAL LAWYER  WILL TRAVEL

Experienced Trial Lawyer Robert Klingler will litigate and try your case for you and share the fee under Ohio Prof. Cond. Rule 1.5.

RK ROBERT A. KLINGLER CO., L.P.A.
ATTORNEYS AT LAW

513-665-9500
rak@klinglerlaw.com