Preparing for compliance: How California's Consumer Privacy Act may impact your clients

April 1, 2019

The California Consumer Privacy Act (CCPA) is a new consumer privacy law that affords California residents increased rights in accessing and controlling how organizations use personal data. Enacted June 28, 2018, CCPA began as a ballot initiative and will become effective January 1, 2020. Organizations that fall within its broad reach need to start thinking about compliance.

So, why should you care about new laws in California? The answer is simple. Organizations based in Ohio or elsewhere may need to comply with the CCPA. (Also, ballot initiatives that start in California often make their way to Ohio. For example, both the Ohio Drug Price Relief Act of 2017 and the Ohio Kidney Dialysis Patient Protection Amendment of 2018 had their genesis as California ballot initiatives.)

Here's what you need to understand about the CCPA.

Who is required to comply with the CCPA?

The CCPA applies to any for-profit entity doing business in California that collects the personal information of California residents, determines the purposes and means of processing the personal information, and meets one of the following criteria:

1) Has gross revenue greater than $25 million

2) Annually buys, receives, sells or shares the personal information of more than 50,000 consumers, households or devices for commercial purposes

3) Derives 50 percent or more of its annual revenues from selling consumers' personal information

The law also extends to any entity that either controls, or is controlled by, a covered business or shares common branding (name, trademark or service mark) with a covered business.

What information is protected under the CCPA?

Personal information is protected. This is broadly defined as information that identifies, relates to, describes, is capable of being associated with or could reasonably be linked, directly or indirectly, with a particular consumer or household. Types of personal information can include names, postal addresses, IP addresses, email addresses, account names, credit card numbers, driver's license numbers, browsing history, geolocation information and other identifying information.

What is required to be disclosed to consumers or deleted under the CCPA?

Covered businesses under the CCPA that collect a consumer's personal information will need to disclose all of the following upon receipt of a verifiable consumer request:

- The categories of personal information collected
- The sources of the information
- The business or commercial purpose for collecting or selling personal information
- The categories of third parties with whom the business shares personal information
- The specific pieces of personal information collected

Businesses that sell or disclose personal information for a business purpose will also have additional disclosure requirements if they receive a verifiable consumer request.

Additionally, covered businesses must delete any personal information they have collected upon a consumer's request, subject to a few exceptions. Such exceptions include data necessary to:

- Complete a transaction or provide a service the consumer requested
- Engage in activities reasonably anticipated within ongoing business with the consumer
- Protect against fraud or other illegal activity
- Comply with the law
- Engage in certain research
- Exercise free speech rights
- Enable internal uses reasonably aligned with consumer expectations

Consumers will have the right to opt-out of allowing a business to sell their personal information to third parties. A business will need to provide a clear and conspicuous link on its website's homepage titled "Do Not Sell My Personal Information." Note that minors between the ages of 13-16 are considered to be automatically opted-out and must affirmatively opt-in for their personal information to be sold.

What else should I know about the CCPA?

The above requirements of the CCPA are not exhaustive and many businesses with an online presence may become a covered business simply from having California residents visit their website. As a result, it is important for organizations that conduct business in California or online to know if the CCPA applies to them.

If the CCPA does apply to an organization, its privacy statements telling consumers how it handles their information and related consumer requests need to be updated to reflect the CCPA's requirements. Also, the organization must adopt compliant internal privacy policies. Failure to comply could result in California Attorney General enforcement actions or private lawsuits.

Privacy compliance is swiftly coming to the forefront in the minds of consumers and legislators at both the state and federal

level. Regularly reviewing and updating an organization's privacy policies is a great step in not only avoiding liability but also instilling confidence in consumers that the organization values their privacy as well as their business.

Authors

Anne Marie Sferra

Partner

Columbus
614.227.2394
asferra@bricker.com

