BROOKS PIERCE

What North Carolina Businesses Need to Know About the California Consumer Privacy Act

10.11.2019

Consumer privacy laws enacted on the other side of the country could have big implications for businesses here in North Carolina. On January 1, 2020, the California Consumer Privacy Act (CCPA) will take effect. This is a sweeping law that applies broadly to any business that collects personal information from California consumers and does business in the state of California. A physical presence in California is not necessarily required to "do business" there—in fact, the law purports to apply to businesses located outside the state.

Given the fast approaching implementation deadline, North Carolina businesses should begin evaluating CCPA and its potential impacts quickly if they have not done so already.

Below is a brief summary of CCPA's main requirements. As will be evident below, CCPA adopts a number of consumer-empowering rights, including rights of notice, rights of access, data deletion rights, and opt-out rights.

Applicability. CCPA generally applies to any for-profit company doing business in California that collects personal information about California consumers and determines the purposes and means of processing that information and falls within one or more of these three categories: they have annual gross revenues greater than $25 million; they buy, collect, sell, or share the personal information of 50,000 or more consumers, households, or devices or they derive 50% or more of annual revenues from selling personal information.

The law also applies to entities that control or are controlled by or share branding with a business meeting the criteria above.

CCPA has exemptions for businesses that are already subject to specific federal privacy regulations. The thresholds for application of the law also mean some smaller businesses are not covered.

Personal Information. CCPA defines "personal information" very broadly as "information that identifies, relates to, describes, is capable of being associated with, or could be linked, directly or indirectly, with a particular consumer or household." It specifically includes typical categories, like name, email address, geolocation data, etc., and some additional categories, like browsing history and audio, electronic, visual, thermal, and olfactory information. Certain publicly available information is excluded.

Notice Requirement. CCPA requires businesses to notify consumers of the categories of personal information collected from them and the purposes for which the personal information will be used *at the time of or before collection*. No new categories of information, and no new uses for previously collected information, may be made without a new disclosure prior to the new collection or new use. This notice is typically provided through a privacy statement or policy.

Right of Access. CCPA permits consumers to request information from businesses about the personal information that may be collected about them and obtain access to the information. Upon a verifiable request, and subject to certain exemptions, businesses are required to disclose and deliver requested information within 45 days. Consumers must be able to request their information through at least two means, including a toll-free number and, if the business has a website, a website link.

Right of Deletion or Right to be Forgotten. Subject to a number of statutory exceptions, CCPA requires businesses to delete, upon verifiable request, any personal information relating to a consumer and direct any service providers with the information to also delete it. There are several important exceptions to data deletion requests, including data necessary to complete a transaction requested by the consumer, data to detect security incidents, and data necessary for research purposes in the public interest.

Opt-Out Right. CCPA requires businesses that sell personal information to permit consumers to opt-out of this selling and to provide notice to consumers of their right to opt-out by disclosing it in their privacy policies. For businesses that sell personal information, a "clear and conspicuous" link titled "Do Not Sell My Personal Information" must be included on the company home page and in the online privacy policy. This link must enable a consumer, or someone authorized on the consumer's behalf, to opt-out of the sale of personal information without requiring the consumer to create an account. (Opt-in rather than opt-out requirements apply for consumers who are minors.)

Equal Terms of Service. CCPA prohibits businesses from discriminating against a consumer because the consumer has exercised any of the rights summarized above. Businesses therefore may not deny goods or services, charge different prices, provide different levels or quality of goods or services, or suggest that the consumer will be treated differently based on the consumer's exercise of rights. However, CCPA does make clear that a business may charge consumers different prices or provide different levels or quality of goods or services if the difference is "reasonably related to the value provided to the consumer by the consumer's data."

Enforcement. CCPA permits a private right of action by consumers in the event of a data breach involving unencrypted or unredacted personal information resulting from a company's failure to maintain "reasonable security procedures and practices appropriate to the nature of the information." Damages may range from $100 to $750 per consumer per incident or actual damages, whichever is greater. The California Attorney General may also bring an enforcement action for violations of CCPA, with civil damages up to $2,500 per violation or, in the case of an intentional violation, up to $7,500 per violation.

As January 1 approaches, North Carolina businesses should consider these actions:

- Evaluate whether CCPA will apply to them based on statutory triggers and exemptions.
- Review and update existing privacy policies to ensure compliance with CCPA and other applicable laws.
- Assess whether employee training is needed to fulfill data access requests, verification processes, and other requirements.
- Assess and implement processes and methods for responding to requests to access and delete personal information and to fulfill opt-out requests.
- If required, comply with the "Do Not Sell My Personal Information" website link and opt-out requirements.
- Evaluate whether data security procedures and practices are "reasonable" and appropriate based on the nature of the personal information collected.

CCPA will in all likelihood set the standard for action by other states looking at privacy legislation. In fact, a number of states have already proposed copycat laws that borrow from CCPA's framework. Even if CCPA does not apply to your business now, the consumer-oriented rights adopted in it may be the new normal. It is not too soon to start planning your compliance strategy.

Brooks Pierce summer associate Morgan Maccherone, UNC School of Law Class of 2021, contributed to this article.

For more information on this legislation, please contact Elizabeth Spainhour, linked below.

PEOPLE

Elizabeth Spainhour

SERVICES

Privacy