SEYFARTH SHAW

Management Alert

The California Consumer Privacy Act of 2018: What Businesses Need to Know Now

By Jason Priebe and John Tomaszewski

California, home to more than 40 million people and the 5th largest economy in the world, has passed the California Consumer Privacy Act (CCPA), its omnibus consumer privacy law. The law creates sweeping new requirements concerning the collection, maintenance, and tracking of information for both employees or customers who are residents of California. Many aspects of the implementation and enforcement are still being finalized by the California Attorney General. However, companies with employees or customers in California need to take stock of the information they are processing that could qualify as "personal information" for California residents, and they need to begin establishing mechanisms for compliance before the end of 2019.

The California Consumer Privacy Act

Effective January 1, 2020, the law applies to businesses collecting, selling, or disclosing personal information in California. In sum, its intended purpose is to require impacted businesses to provide enhanced transparency and to give consumers the right to control their personal information. Specifically, its goal is to further a California consumer's right to privacy by ensuring various rights including: 1) knowing what personal information is being collected; 2) knowing whether their personal information is sold or disclosed and to whom; 3) saying no to the sale of their personal information; 4) access to their personal information; and 5) equal service and price, even if they exercise their personal rights.

What Companies Are Affected?

The CCPA applies to any company doing business or with employees in California if they:

- generate $25 million or more a year in revenue;
- annually buy, receive, sell, or share personal information of 50,000 or more consumers, households, or devices for commercial purposes; or
- derive 50% or more of their annual revenue from selling consumer personal information.

Its Implications and Why It's Important

First, several terms integral to the law's application are given broad stroke meaning. These terms: 1) determine which organizations must comply with the law; 2) determine the scope of what is considered personal information; 3) determine

whose personal information the law applies to; and 4) acknowledge personal information as an asset through a broad definition of 'sell.' These terms include:

1. **Business** is defined as any company that does business in California for a profit that collects *personal information* and that either (i) has annual gross revenue more than $25 million; (ii) annually buys, *sells*, receives, or shares for a commercial purpose the personal information of 50,000 or more consumers, households, or devices; or (iii) derives 50% or more of its annual revenues from *selling* consumer's personal information. Note that both "sell" and "personal information" are integral parts of the definition of business.

2. **Personal information** is defined to include anything that identifies, relates to, describes, is capable of being associated with, reasonably linked, directly or indirectly, with a particular consumer or household and includes, *but is not limited to*, such things as:

   > Individual Identifiers such as real name, alias, postal address, unique personal identifier, Internet Protocol Address, email address, account name, social security number, passport number, or other similar identifiers; Geolocation data; Biometric Information; Internet or other electronic network activity; Audio, electronic, visual, thermal, olfactory, or similar information; Inferences that can be drawn from any of the previous information in order to create a profile; and the list goes on.

3. **Consumer** is defined as a natural person who is a California *resident* including by any *unique identifier*. (*NOTE: Resident means* (1) every individual who is in the state for other than a temporary or transitory purpose and (2) every individual who is domiciled in the state who is outside the state for a temporary or transitory purpose. All other individuals are nonresidents.)

4. **Sell** or variants of the word means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by one covered business to another business or a third party for monetary or other valuable consideration.

Together, these terms, along with other definitions, as applied to legal requirements under the law, result in compliance obligations for many organizations doing business in California.

Second, under the CCPA, the state legislature has tasked the California Attorney General with the primary responsibility to enforce its provisions. As its enforcement arm, the Attorney General has various enforcement mechanisms at its disposal. For example, this includes the ability to penalize non-compliant organizations through administrative fines upon the expiration of a 30 day notice of violation and opportunity to correct. These fines may not exceed $2,500 per violation or $7,500 for intentional violations.

More importantly, the Attorney General has the authority to decide how organizations must comply. In the above example, this could include defining what constitutes a violation. Depending on how the Attorney General defines a violation, it could result in vastly different penalties. Given that the law has just passed, it is unclear how the Attorney General will enforce the statute or determine whether a violation has taken place for a particular situation. That said, the law gives the Attorney General broad discretion to make those determinations."

Actions Required

What Companies Conducting Business in California Need to Know

Despite an effective date of January 1, 2020, for an impacted California business to be in compliance, companies are advised to begin coordination efforts to comply far sooner than this because of the complexity of the law.

In addition to taking certain steps to be in compliance and reinforcing consumer rights regarding the privacy of personal information businesses must:

- Perform a data inventory in order to identify informational flow. Following completion, the business will need to identify issues impacting compliance and develop controls or countermeasures to address them.
- Provide California consumers with two or more methods for submitting their requests for information—including, at a minimum, a toll free telephone number.
- On its online privacy policy or policies (if in existence) or otherwise on its website, disclose a description of a consumer's rights pursuant to this law regarding the collection, use, and sale of personal information and one or more designated methods for submitting requests, and provide a list of the categories of personal information it has collected, disclosed for a business purpose, or sold in the preceding 12 months by reference to specific categories of personal information in the law—or if the business has not done so, to disclose that fact. Information so posted must be updated at least once every 12 months.
- On its website home page, provide a link to a web page titled 'Do Not Sell My Personal Information' in order to allow a customer (or their agent) to opt out on the sale of their personal information to a third party. In addition to this link, the business is required to include a description of a consumer's rights, along with a separate link to the above titled 'Do Not Sell My Personal Information' page in its online privacy policy or policies (if in existence) as well as any California-specific description of consumers' privacy rights.
- Implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information.

Jason Priebe is a partner in Seyfarth Shaw's Chicago office, and John Tomaszewski is a partner in Seyfarth Shaw's Houston office. This Management Alert is not intended to provide an exhaustive list of concerns an impacted business may encounter with the California Consumer Privacy Act. If you have any questions, please contact Jason Priebe at jpriebe@seyfarth.com or John Tomaszewski at jptomaszewski@seyfarth.com.