California Passes New Data Privacy Law With National Implications

Written by Colin J. Zick, Christopher Escobedo Hart

July 17, 2018

The California Consumer Privacy Act of 2018 (the "CCPA") was signed into law on June 28, 2018. Although it is a state law, it has national and international ramifications. Here are some key aspects to be aware of.

1. Effective date

The law is slated to go into effect on January 1, 2020. However, the California State Legislature has the option of offering amendments to alter the law between now and its effective date, and amendments are expected. Additionally, the California Attorney General is specifically authorized to adopt regulations to further the statute's purpose. So when assessing your obligations and working toward compliance, keep in mind that the specific contours of the law are subject to change, and as yet unwritten regulations (as well as California AG guidance) will shed further light on how the law will be implemented and enforced.

2. Overall approach

Similar to the General Data Protection Regulation (GDPR) that recently went into effect in the European Union, the CCPA begins from the starting point of data privacy as a fundamental right (rather than, in most cases in U.S. law, as a balance between consumer and business interests). A rights-based approach to data privacy not only frames the content of the law, but can also affect its interpretation, potentially leaning in favor of protecting the individual even in the face of otherwise reasonable company actions (reasonableness is often a touchstone in U.S. data privacy laws).

3. Scope

The CCPA does not apply to all private entities. In only applies to an entity doing business in California that either (1) has annual gross revenues over $25 million, (2) annually buys, receives, sells, or shares the personal information of 50,000 or more California residents, households, or devices, or (3) derives 50% or more of its annual revenue from selling personal information of California residents.

To the extent the CCPA does apply, the scope will be broad. Similar to the GDPR (and distinct from most state data privacy laws), "personal information" is broadly defined. It is 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." This can include a name, address, IP address, or email account, as well as biometric and geolocation information.

4. Unique obligations

Similar to the GDPR, but unique in U.S. law, the CCPA provides for the following individual data privacy rights:

a. The right to know the purpose of data collection and what categories of personal data are being collected before the collection takes place.

b. The right to object a company's sale of a consumer's personal information.

c. The right for additional information regarding the personal information being collected.

d. The right to have one's personal information deleted (with exceptions).

e. The right to know whether one's personal information is disclosed to a third parties (and to know which third parties information is disclosed to).

f. The right to not be discriminated against in terms of the price of a company's services in the event an individual chooses to exercise his or her privacy rights.

As a practical matter, after determining whether the law applies to your company, the compliance questions will involve data mapping and creating procedures for complying with requests from consumers, as well as updating your company's privacy policy. If your company has already taken these actions with regard to GDPR compliance, much of this work will transfer over to compliance with the CCPA.

5. Liability

The CCPA vests enforcement authority in the California Attorney General, which can impose a fine of $2,500 per negligent violation (violations go beyond data breaches and include not complying with an individual's data privacy rights), and $7,500 per intentional violation, and also provides a limited private right of action to individuals for data breaches (which can include actual damages or set damages of up to $750 per consumer per incident).

***

In sum, the passage of the CCPA is a seismic event in U.S. data privacy law. While the scope of the law might change between now and its effective date, the future of U.S. data privacy law seems clearly to be trending in the direction of a more expansive, rights-based approach to privacy. Those companies that have already done the work of being GDPR compliant are a step ahead; the CCPA suggests that many other companies will have to follow suit.

RELATED PRACTICES

- Privacy & Data Security
