June 29, 2018

California Passes Consumer Privacy Act

On Thursday, June 28, 2018, Governor Jerry Brown signed into law the California Consumer Privacy Act of 2018 (the "CCPA"), which may significantly impact many companies that collect and monetize personal data from California residents. Among other things, the law, which applies only to the data of California residents ("consumers"), would require companies to give consumers information about what data they collect and sell, as well as to delete data about consumers if requested in some circumstances. If the company sells data about consumers, the law would also permit consumers to opt out of that practice. Additionally, in some contexts, the CCPA would provide consumers with a private right of action in the event their data is subject to an unauthorized access, theft, or disclosure as the result of the company's failure to implement and maintain "reasonable security procedures." The CCPA is scheduled to come into effect on January 1, 2020, and, given the length of time before the effective date and the rush to pass the bill, it is likely that additional modifications will be made. A bill passed by the legislature is easier to amend than a ballot initiative.

The CCPA is the result of a last-minute compromise agreement between California lawmakers and Californians for Consumer Privacy, the activist organization behind a data privacy ballot initiative (also entitled the California Consumer Privacy Act) that was widely criticized by businesses as broad and unworkable. Indeed, if passed into law, the ballot initiative would impose formidable compliance challenges while significantly increasing litigation risk for businesses subject to the law. With over 600,000 signatures, the ballot initiative was approved to appear on the November ballot on Monday. Per the agreement, the ballot initiative was withdrawn.

The Statute

The potentially broad reach of the CCPA is underscored by its definition of personal information, which expands far beyond traditional identifiers such as name, address, and social security number. Under the CCPA, "Personal Information" encompasses any information that "identifies, relates to, describes, is capable of being associated with" or that could "reasonably be linked, directly or indirectly, with a particular consumer or household." Personal information protected by the act includes, for example, biometric data, internet activity, and consumer profiles based on inferences from various bits of data. The definition is similar (but not identical) to the definition of "personal data" contained in the EU's General Data Protection Regulation ("GDPR"), which has been noted for its breadth. Unlike the GDPR, however, the CCPA excludes from its definition information that is publicly available. Any company that collects data from California residents should closely analyze whether that data meets the CCPA's unconventional conception of "personal information."

The CCPA would establish certain "rights," some familiar to Europeans, such as the so-called "right to be forgotten." The CCPA requires businesses to delete personal information about a consumer at the consumer's request, provided the data is not necessary for specified purposes, including to complete the transaction or provide other goods and services within the scope of an ongoing business relationship with the consumer, to comply with legal obligations or to enable other internal uses by the business that are "reasonably aligned with the expectations of the consumer," based on their relationship with the business.

Among other "rights" established by the CCPA are the right to request details about the personal information the business has collected, such as the categories of sources of the data and the categories of third parties with whom the data will be shared. Businesses that collect personal information are required to inform consumers about the categories of information collected and the purposes for which such data will be used at or before the point of collection. Consumers could also request disclosures about whether the business sells or discloses their data, and

would have the right to opt out of any such sales. While the CCPA expressly prohibits companies from discriminating against customers who choose to exercise these rights, the bill does not prohibit a business from charging a consumer a premium, provided the premium is a reasonable price and is related to the "value provided to the consumer by the consumer's collected data" (an awkward phrase, discussed further below).

Businesses can also expect another round of revisions to their privacy policies, as the CCPA requires that covered businesses update their privacy policy to include descriptions of the new consumer rights, the methods for submitting requests, and the categories of personal information that it collects, sells, or discloses for a business purpose. Businesses that have "actual knowledge" that a consumer is under the age of 16 are prohibited from selling personal information about that consumer unless the consumer (or, in the case of children under the age of 13, their parent or guardian) opts in.

Enforcement

One feature of the CCPA receiving significant attention is its creation of a private right of action for California residents whose unencrypted "personal information" is subject to unauthorized access, exfiltration, theft, or disclosure "as a result of" a failure by the company to institute "reasonable" security procedures and practices. The CCPA provides for statutory damages of between $100 to $750 per consumer per incident, or actual damages if greater. However, the meaning of "personal information" for purposes of the private right of action is limited to the more traditional identifiers contained in California's data security statute, such as name, social security number, and credit card information, rather than the broad definition of "personal information" used elsewhere in the CCPA.

Additionally, there are further limits imposed on the right of action. First, the CCPA requires would-be plaintiffs to provide businesses with 30 days' written notice of the alleged violation before filing suit and precludes an action if the business cures the alleged violation in that time frame. Second, plaintiffs would have to provide notice of any action to the California Attorney General, who would have the authority to notify the consumer that he or she must not proceed on the action.

Notably, unlike the proposed ballot measure, the CCPA does not create a private right of action for violations of other provisions of the statute. Instead, civil penalties for violations of the statute would be exclusively assessed and recovered in civil actions brought by the California Attorney General. The proposed ballot measure also provided for whistleblower actions, which are not included in the CCPA.

Exceptions

The CCPA's scope is limited by several exceptions. First, the law only applies to businesses that (1) have revenues of over $25 million; (2) buy, sell, or receive for the business's commercial purposes personal information about 50,000 or more customers; or (3) derive more than 50 percent of their annual revenue from selling consumers' personal information. Second, the law does not restrict the processing of "deidentified" data or aggregate consumer information. Deidentified data is data that cannot reasonably identify or be linked to the individual, directly or indirectly, provided that the business has instituted safeguards to prevent any such re-identification. Third, the law does not impact the processing of data if both the consumer and the conduct at issue occur outside of California. Fourth, the law does not apply to health information governed by HIPAA. Other carve-outs include the collection or use of data to comply with other laws or to cooperate with law enforcement, processing of personal data covered by Gramm Leach Bliley, to the extent there is a conflict between the laws, and the sale of information to or from a consumer reporting agency covered by the Fair Credit Reporting Act.

Looking Ahead

Although the CCPA is not scheduled to become effective until 2020, companies potentially subject to it should begin to evaluate how it might impact their operations. Perhaps reflecting the rushed manner in which the legislation was adopted, there remains considerable ambiguity about some key provisions within the Act. For example, as discussed above, companies are not permitted to discriminate against consumers who exercise their rights under the Act through differentiated pricing or lower service levels. However, the Act provides that companies may offer a

different price if the consumer allows the company to sell their data, provided the price difference is "directly related to the value provided to the consumer *by the consumer's data*." Presumably, this is intended to mean the value provided to the consumer in exchange for their data, but on its face, it would appear that companies are required to calculate the intrinsic value to the consumer of their personal information.

Many of these ambiguities could be resolved through regulation, and since the Act was passed quickly in order to head off a similar ballot initiative, without significant debate, it is expected that the legislature may consider future modifications. Ropes & Gray will continue to closely monitor developments.

For more information about the CCPA or to discuss privacy or cybersecurity practices generally, please feel free to contact a member of Ropes & Gray's leading privacy & cybersecurity team.