May 13, 2019

Preparing for the California Consumer Privacy Act in an Evolving Privacy Landscape

Just a month after the European Union's General Data Protection Regulation (GDPR) took effect, California enacted the most expansive data privacy law in the United States to date. The California Consumer Privacy Act (CCPA), which is scheduled to go into effect on January 1, 2020, will impose unprecedented data obligations on companies doing business in California, requiring increased data use transparency and the observance of novel consumer data rights. Notwithstanding any GDPR compliance fatigue, companies need to take steps to prepare for compliance with the CCPA.

The CCPA was a hastily crafted legislative package passed to preempt a statewide ballot initiative set to qualify for California's November 2018 ballot. The initiative—which promised to be even more far-reaching—was withdrawn by its ballot sponsors in exchange for passage of the CCPA. The statute remains a work in progress, with numerous legislative amendments currently under consideration and implementing regulations from the California Attorney General expected this fall.

Scope. The CCPA applies to all for-profit entities with over $25 million in annual gross revenue that do business in California and collect (or engage a third party to collect) the Personal Information ("PI") of California residents, defined broadly as any 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." As the statute applies to individuals domiciled in California even if located out-of-state when their PI is gathered, companies will likely find it difficult to target compliance geographically.

Compliance Requirements. The CCPA's requirements are extensive and diverge significantly from those imposed by the GDPR. To comply, companies that collect PI of California residents (wherever located) must:

- Disclose, upon consumer request, the use of the consumer's PI, including what PI is being collected, sold, or disclosed, the PI's source, its business purposes, and the categories of third parties to which the PI is disclosed;
- Honor consumer requests to delete PI, including directing service providers or other third parties to honor requests through deletion;

- Provide consumers with the ability to opt out of sale of their PI through a clear and conspicuous link on the company's homepage titled "Do Not Sell My Personal Information," as well as a link to relevant privacy policies;
- Update privacy policies, including by describing the consumer's CCPA rights and providing a list of categories of PI collected, sold, or disclosed;
- Refrain from discriminating against consumers with respect to prices or services based on their exercise of CCPA rights; and
- Implement and maintain "reasonable security procedures and practices" to protect and safeguard consumer PI.

Remedies. The California Attorney General can impose fines that include damages of up to $7,500 for each intentional violation (and $2,500 for each unintentional violation), if not cured within 30 days. In addition, the CCPA provides consumers with a private right of action; while the right is currently limited to the data breach context, a bill pending in the legislature, supported by the Attorney General, would expand that right to apply to any CCPA violation.

Considerations. Companies should carefully assess the impact of the CCPA on their businesses, including through:

- Review of data practices, with a particular focus on collection, sale, and disclosure of consumer PI;
- Investment in infrastructure needed to deliver on the consumer rights created by the CCPA; and
- Due diligence regarding counterparties' CCPA compliance, particularly in connection with critical transactions, such as mergers and acquisitions.

The CCPA marks the first sweeping change to the data privacy regulatory landscape in the United States, but it will almost certainly not be the last: a dozen states and the U.S. Congress are considering bills modeled on the CCPA or the GDPR. Companies must not only monitor ongoing legislative and regulatory developments closely, but they should invest in data privacy compliance programs with the flexibility to adapt and scale to meet shifting requirements in a rapidly evolving data privacy environment.

David A. Katz
Marshall L. Miller
Zachary M. David