WINSTON & STRAWN LLP

CLIENT ALERT

New California Law Introduces Additional Regulation of Consumer Information

JULY 3, 2018

Background

California has become the first state to make significant changes to its privacy scheme in the context of the recently implemented European Union's General Data Protection Regulation (GDPR). The California Consumer Privacy Act of 2018 (CCPA) goes into effect on January 1, 2020, and it will rank amongst the most stringent privacy laws in the United States for those companies that fall under its purview. The sweeping new law will provide California residents with more control over their personal information and provide significant penalties to covered companies that fail to comply.

Protected Information

The CCPA includes a broad definition of what constitutes "personal information." Many other US state privacy laws limit their definitions of "personal information" to certain identifiers that could be used to commit identity theft (e.g., consumer names in combination with Social Security numbers or financial account numbers). However, the CCPA mimics GDPR in applying to 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."

Scope of Application

The scope of the CCPA is limited to companies that conduct business in California; collect, or have collected on their behalf, the personal information of California residents; and satisfy at least one of the following:

- Produce annual gross revenues in excess of $25,000,000;
- Alone or in combination, annually buy, receive for their own commercial purposes, sell, or share for commercial purposes the personal information of 50,000 or more consumers, households, or devices; and/or
- Obtain 50% or more of their annual revenue from selling, releasing, renting, or otherwise making available consumer personal information to a third party for monetary or other valuable consideration.

Note, the new law does not apply to information already regulated under the Health Insurance Portability and Accountability Act, the Graham-Leach Bliley Act, the Fair Credit Reporting Act, or the Drivers' Privacy Protection Act.

Protections and Obligations

As a practical matter, the CCPA will impose a number of significant changes to the business practices of companies that fall under its purview. Namely, with respect to a consumer's own personal information, the CCPA empowers consumers to (with some exclusions):

- Request that a company to disclose what personal information the company has collected and/or sold;
- Instruct a company to refrain from selling personal information;
- Request that a company delete personal information (which is similar to the GDPR's "right to be forgotten"); and
- File a regulatory complaint or bring a private action against a company that fails to secure personal information or otherwise violates the provisions of the CCPA.

The CCPA also expands the required privacy disclosures that companies are required to give when collecting or using consumers' personal information (e.g., in a website or mobile application privacy policy). These disclosures now must include a description of the rights California residents have about their personal information (as outlined above) and how they can exercise such rights, as well as detailed information about how companies collect, use and share personal information. In addition, companies must provide a link to a "Do Not Sell My Personal Information" page that is accessible on relevant platforms, with an opt-out mechanism for consumers. Moreover, as with GDPR, the CCPA prevents organizations from denying services or products to individuals that choose to exercise their rights under the CCPA or refuse to provide consent.

Enforcement

The CCPA includes mechanisms for both consumers and California regulators to bring suit for violations. Consumers may file complaints with the California Attorney General, or in certain circumstances, file their own lawsuits, for potential violations of the CCPA. The law provides for penalties of up to $7,500 for each violation.

In addition, the CCPA contains a provision that allows consumers whose personal information is stolen, or impermissibly accessed, exfiltrated or disclosed to bring suit against companies for failing to protect their information. For these suits, the statutory damages range from $100 to $750 per consumer. Interestingly, this provision of the CCPA does not appear to track with California's existing security breach notification law, which provides a separate standard for what constitutes a security breach.

For companies subject to the CCPA, there may be more requirements to come. The law gives the California Attorney General the authority to create implementing regulations and there is additional "cleanup" legislation expected. While awaiting further guidance on this front, companies can begin to circle-up internally with their business teams to better understand how personal information is collected, used and shared. This will enable companies to both assess whether the CCPA will apply to them and to put some initial thought into how business practices may need to be adjusted or created in order to meet their obligations under the CCPA.

For more information, please contact: Alessandra Swanson, Steve Grimes, John Rosenthal, Eric Shinabarger

3 Min Read

Related Locations

Charlotte | Chicago | Dallas | Houston | Los Angeles | New York | San Francisco | Silicon Valley | Washington, DC

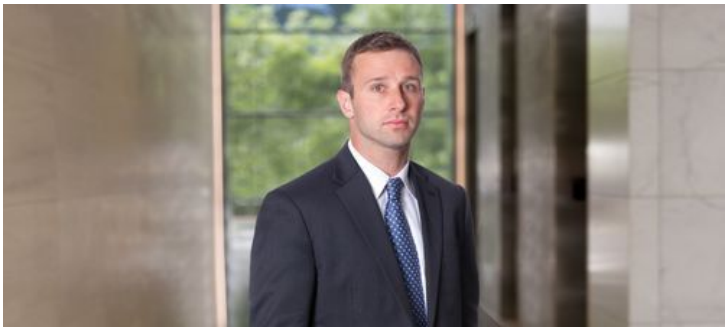
Related Capabilities

Privacy & Data Security

Related Regions

North America

Related Professionals



Steven Grimes

John Rosenthal

Eric Shinabarger

Alessandra Swanson