IP Alert: GDPR Arrives in the U.S. – The 2018 California Consumer Privacy Act

July 18, 2018

California is once again at the vanguard of privacy law in the U.S.A. On June 28, 2018, hot on the heels of the May 25th effective date of the European Union's General Data Protection Regulation (GDPR), California passed the United States' broadest privacy law to date. The 2018 California Consumer Privacy Act (CCPA) mirrors some of the GDPR's stringent data protection requirements and will require many U.S. businesses to adjust their current data collection practices. While CCPA only applies to personal information of California residents, it will likely have much broader implications. Although CCPA does not go into effect until January 1, 2020 and will likely go through several revisions before the effective date, it may become the de facto national standard for how businesses use personal information to market their products and services. The cost, complexity, and difficulty of maintaining a different set of privacy procedures for California residents may be impractical and other states may follow the California model.

CCPA was passed quickly following an agreement with a consumer privacy organization to withdraw a broader privacy initiative that would have appeared on the November ballot. The withdrawn initiative would have granted additional private rights of actions to consumers. CCPA still provides consumers new privacy rights and mandates certain disclosures from businesses regarding the use and sale of personal information.

Personal Information Under CCPA

The definition of personal information under CCPA is extremely broad and includes 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." Personal information includes personal identifiers such as names, email addresses, social security numbers, biometric information, internet activity information, browsing history, search history, geolocation data, purchasing or consuming history, professional or employment-related information, education, and any "inferences drawn from any of the information."

Who Needs to Comply?

CCPA applies to any business that collects personal information from California residents and:

- Has annual gross revenues of $25 million or more;
- Buys, receives, sells, or shares the personal information of at least 50,000 California residents, households, or devices annually; or
- Derives a minimum of 50% of its annual revenue from selling California residents' personal information.

Disclosures and Opt-Out

Consumers have the right to opt-out of the sale of their personal information and businesses are required to notify consumers of this right. Businesses must also list the categories of information collected about consumers in the past 12 months and identify whether the business sells or discloses that personal information. These disclosures must appear in the business' online privacy notice.

Furthermore, businesses may have to include a clear and conspicuous link on their website stating "Do Not Sell My Personal Information." Consumers must be able to use this link to opt-out of the sale of their personal information. In addition, a business cannot discriminate against consumers because they exercise their right to opt-out of the sale of their personal information or for exercising any other rights provided under CCPA.

Right to Deletion

Similar to the GDPR requirement that businesses erase or delete certain personal information, California residents will now have the right to request deletion of their personal data. Except for certain circumstances, a business must delete the personal information it holds about a consumer upon that consumer's request. Businesses may need to update their internal processes and data systems to respond to such requests in a timely fashion.

Enforcement

CCPA is enforceable by the California Attorney General and authorizes a civil penalty of up to $7,500 per violation. California residents have a private right of action under CCPA only when unencrypted information is accessed during a data breach. This increases the importance of having appropriate incident response plans in place to handle a potential data breach. The withdrawn privacy initiative would have provided more

private rights of action by consumers.

Outlook

While the 2018 California Consumer Privacy Act and the recently implemented GDPR provide legal incentive for businesses to strengthen their privacy practices, these laws are indicative of a shift in consumer expectations that goes beyond mere compliance with the law. Data breaches are increasingly common and consumers are more focused on privacy and personal data protection than ever before. Businesses that take a holistic approach to privacy and establish strong privacy practices now will not only be well poised to comply with CCPA and other privacy laws, but will also have a competitive advantage in the marketplace.

For now, businesses should begin performing data mapping as necessary to inventory the personal information they collect on California residents, households, and devices. Businesses should also be implementing internal policies and procedures for handling data access requests to ensure these requests can be adequately complied with by the effective date. Incident response plans should be in place to handle data breach notification requirements. Further, businesses should update their privacy policies with new disclosures regarding data access and deletion.

The California attorney general has been tasked with the promulgation of regulations as necessary to implement CCPA and there will likely be significant lobbying to amend and clarify provisions of CCPA.

We will continue to monitor CCPA, the GDPR, and other data privacy laws to advise our clients on best practices in this evolving area of the law.

For more information, contact Michael Cohen or Amanda McAllister of the Gray Plant Mooty Intellectual Property, Technology, and Privacy team.