Privacy/Data Breach

In June of last year, Governor Jerry Brown signed into law the California Consumer Protection Act of 2018 (CaCPA). CaCPA applies to any entity that does business in California and satisfies one or more of the following: (i) annual gross revenue in excess of $25 million; (ii) alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; OR (iii) derives 50% or more of its annual revenues from selling consumers' personal information. Under CaCPA, key consumer rights include:

- The right to request deletion of personal information which would require the business to delete information upon receipt of a verified request;
- The right to request that a business that sells the consumer's personal information, or discloses it for a business purpose, disclose the categories of information that it collects and categories of information and the identity of any third parties to which the information was sold or disclosed; and
- A consumer's right to opt-out of the sale of personal information by a business prohibiting the business from discriminating against the consumer for exercising this right, including a prohibition on charging the consumer who opts-out a different price or providing the consumer a different quality of goods or services, except if the difference is reasonably related to value provided by the consumer's data.

At the end of August 2018, several substantive amendments to the CaCPA were enacted. These amendments provide:

- A clarification to the definition of personal information: The data elements listed in the definition are personal information, not automatically, but to the extent that they identify, relate to, describe, are capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household;
- An expansion of exempt information to include protected health information collected by a business associate governed by HIPAA/HITECH;
- A clarification that personal information governed by the Gramm-Leach-Biiley Act, the California Financial Information Privacy Act, and the Driver's Privacy Protection Act of 1994 is exempt regardless of whether the CaCPA conflicts with these laws;
- A clarification that information collected pursuant to the Gramm-Leach-Biiley Act and the Driver's Privacy Protection Act of 1994 will not be exempt from a consumer's cause of action relating to certain data breaches;
- A clarification that a private cause of action exists only for data breaches;
- Incorporation of a provision that businesses, service providers, or persons who violate the CaCPA and fail to cure such violation within 30 days will be liable for a civil penalty under the laws relating to unfair competition in an action brought by the state Attorney General; and
- A provision that the state Attorney General will not bring an enforcement action under CaCPA until six months after publication of the final implementation regulations or July 1, 2020, whichever is sooner.

A flurry of additional amendment activity followed through the end of the legislative session on September 13, 2019, with a number of additional amendments heading to Governor Newsom, including a temporary B2B exemption and a temporary notice requirement to employees. Read more about that here and be on the lookout for a comprehensive set of CaCPA FAQs. With an effective date of January 1, 2020, businesses and their service providers should be taking steps to become compliant.

Following on the heels of the European General Data Protection Regulation (GDPR) (See Does the GDPR Apply to Your U.S. Based Company?) and the BIPA class actions discussed above, the CaCPA is a reminder that data privacy protection initiatives are spreading across the U.S. and the globe. Brazil, India, Indonesia, and the Cayman Islands recently enacted, upgraded, or drafted comprehensive data protection laws. Last May, Vermont passed a law requiring data brokers to implement a written information security program (WISP), disclose to individuals what data is being collected, and permit individuals to opt-out of the collection. Last April, the Chicago City Council introduced the Personal Data Collection and Protection Ordinance, requiring opt-in consent from Chicago residents to use, disclose, or sell their personal information. Last fall, San Francisco adopted the "Privacy First Policy," an ordinance requiring that businesses disclose their data collection policies to consumers as a predicate for obtaining city and county permits or contracts. On the federal level, several legislative proposals are being considered to heighten consumer privacy protection, including the Consumer Privacy Protection Act and the Data Security and Breach Notification Act.

Given this legislative climate, it is important that organizations continue to develop a set of best practices to ensure the privacy and security of the personal information they collect, use, or store. Key to this process is creating a data inventory to identify what personal information is collected, how it is used, where it is stored, and when it is destroyed. Once this "data mapping" is completed, attention should be paid to drafting and implementing a WISP. WISPs detail the administrative, technical, and organizational policies and procedures an organization has in place to safeguard the privacy and security of its data. These initial steps will help any organization identify and streamline its data processing activities, reduce its exposure in the event of a data breach, and prepare itself for upcoming data protection legislation.