FLASTER GREENBERG
Attorneys at Law | A Professional Corporation

Cybersecurity & Data Privacy Legislative Updates

Legal Alert

April 9, 2021

Since the passage of the CCPA in 2018, there has been a flurry of proposed state laws aimed at regulating the areas of cybersecurity and data privacy in the absence of federal comprehensive legislation. Additionally, there has been a renewed focus on legislation at the federal level. Here's an overview of some recently proposed pieces of federal legislation, and recently proposed and passed state laws that may actually have a shot at success.

Federal Privacy Legislation

Information Transparency and Personal Data Control Act (2021)

This Act is the first of its kind to be introduced in 2021. The Act would create protections for the processing of personal information. Under the Act, businesses would be required to utilize an opt-out consent mechanism for consumers for the collection, processing, and sharing of non-sensitive information. For the collection, sale, sharing, or other disclosure of sensitive personal information, however, companies would be required to obtain an "affirmative, express, and opt-in consent" from consumers.

The proposed law defines "sensitive personal information" as financial account numbers and authentication credentials, such as usernames and passwords; health information; genetic data; any information pertaining to children under the age of 13; Social Security numbers and any "unique government-issued identifiers;" precise geolocation information; the content of oral or electronic communications, such as email or direct messaging; personal call detail records; biometric data; sexual orientation, gender identity or intersex status; citizenship or immigration status; mental or physical health diagnoses, religious beliefs; and web browsing history and application usage history.

Notably, information that is classified as deidentified, public information, and employee data would not fall under the definition of "sensitive personal information." Written or verbal communication between a controller and a user for a transaction concerning the provision or receipt of a product or service would also not be considered sensitive data.

Additionally, data controllers would be responsible for informing processors or third parties about the purposes and limits to the specific consent granted but would not be liable for processors' failure to adhere to those limits.

Moreover, the law would provide additional rulemaking authority to the Federal Trade Commission to devise requirements for entities that collect, transmit, store, process, sell, share, or otherwise use the sensitive personal information of members of the public.

This Act would not provide consumers with a private right of action. Instead, it directs the Attorney General to notify controllers of alleged violations and provide them with 30 days to cure non-willful violations of this Act before commencing an enforcement action.

For more information on recently-proposed federal legislation, including those crafted to address the COVID-19 pandemic, *see* my pieces on the Exposure Notification Privacy Act, The Public Health Emergency Act, and the COVID-19 Consumer Data Protection Act.

State Privacy Legislation

Unlike comprehensive national laws like the GDPR, which generally applies to all data in all settings, state laws in the U.S. typically carve out exceptions for certain types of data, such as health information already subject to HIPAA, for example. The laws outlined below largely follow this pattern.

The following states have recently passed, or proposed, cybersecurity and data privacy laws.

The CPRA is a ballot initiative that amends the CCPA and includes additional privacy protections for consumers. It was passed in November 2020 and the majority of the provisions therein will enter into force on January 1, 2023 with a look-back to January 2022.

Virginia's law is similar to the still-pending Washington Privacy Act and includes provisions that are akin to the CCPA.

Other states like Oregon and Minnesota have also proposed privacy and security legislation in recent months.

Don't forget to catch Krishna Jani's presentation at PBI's upcoming Cyberlaw Update on Thursday, April 29, 2021!

Krishna A. Jani, CIPP/US, is a member of Flaster Greenberg's Litigation Department focusing her practice on complex commercial litigation. She is also a member of the firm's cybersecurity and data privacy law practice groups. She can be reached at 215.279.9907 or krishna.jani@flastergreenberg.com.