March 29, 2019

What's trending on NP Privacy Partner

The FTC released its Privacy & Data Security Update: 2018 and data privacy legislation updates from Washington State and Washington, D.C. Here's what's trending in data privacy and cybersecurity.

Consumer Privacy

FTC releases summary of 2018 privacy and data security enforcement and outreach

On March 15, 2019, the Federal Trade Commission (FTC) released its Privacy & Data Security Update: 2018, a report summarizing its work on these topics in calendar year 2018.

The FTC, as the body charged with enhancing competition and protecting consumers, detailed its efforts over the past year to attempt to stop privacy and security violations and to require companies to remediate any unlawful practices.

The report highlights the FTC's notable enforcement actions last year, including a settlement with PayPal, Inc. addressing allegedly deceptive privacy settings in its Venmo service line, as well as a judgment exceeding $700,000 against Alliance Law Group for alleged collection of fake debts by individuals posing as attorneys. It also summarizes settlements obtained with VTech Electronics Limited and Explore Talent for alleged violations of the Children's Online Privacy Protection Act (COPPA).

In addition to enforcement actions, the Update discusses the FTC's outreach efforts last year, including the various types of guidance and educational materials promulgated by the FTC in 2018, addressing topics such as cybersecurity tips for small businesses and items for consumers to consider prior to using Virtual Private Network (VPN) apps. It also mentions hearings hosted by the FTC on data security, competition and consumer protection issues surrounding the use of artificial intelligence, algorithms and predictive analytics and privacy and competition issues related to big data.

The Update also discusses reports issued by the FTC in 2018, including one addressing the complex nature of patching mobile operating systems and one highlighting key points from the FTC and National Highway Traffic Safety Administration's workshop on connected cars.

On an international level, the Update details the FTC's engagement with international organizations, privacy authorities in other countries and global privacy authority networks on mutual enforcement of privacy and security requirements, as well as investigation cooperation.

The Update illustrates that 2018 was an active year for the FTC. Given enforcement action and FTC community outreach thus far in 2019, we do not expect that trend to decrease this year. Businesses should ensure that their privacy and security practices remain compliant with the FTC Act and any other applicable laws and regulations governing their industry. In particular, entities should review their privacy policies to ensure that the terms of these documents remain in line with their privacy practices and are not misleading to consumers.

The FTC Privacy & Data Security Update: 2018 can be found here. –*Valerie Breslin Montague*

Cybersecurity

Data privacy legislation updates from Washington State and Washington, D.C.

While there has not been any concrete movement on a federal data privacy law, there has been some progress on the state and local level.

Washington State

Washington State Senator Reuven Carlyle's privacy bill, introduced back in mid-January, cleared the State Senate earlier this month and is under consideration in the House. The bill covers companies that control personal data of 100,000 or more Washington residents and also data brokers with information on at least 25,000 Washington state residents

Some of the obligations imposed on these covered entities echo the CCPA and the GDPR. For instance, companies much specify how they use their personal information and for what purposes. They must also comply with consumer requests to delete personal data, so long as requisite conditions are met (e.g., if a company can no longer identify a business reason for keeping that information). Finally, companies have to perform risk assessments of their data processing activities and take stock of any potential harm for consumers' personal data.

But, other obligations are unique: this bill expressly addresses facial recognition technology. In the bill's current form, any company that uses facial recognition in a public space must give notice to visitors that the technology is in use. Moreover, companies that sell facial recognition software must make their software available for third-party testing to monitor bias. Finally, the bill expressly bars public agencies from tracking individuals using facial recognition without a warrant.

Washington, D.C.

Last week, Washington, D.C., Attorney General Karl A. Racine introduced an amendment to D.C.'s current data breach notification law. Racine's bill expands the definition of personal information to include passport numbers, taxpayer identification numbers, military ID numbers, health information, biometric data, genetic information and DNA profiles and health insurance information. Further, data breach notices to consumers would now have to include (a) categories of information that were, or are believed to have been, involved in the breach; (b) contact information for both the person making the notification and for credit reporting agencies, the FTC and the D.C. Attorney General; and (c) the right under federal law to obtain a security freeze at no cost and how to obtain such a freeze. If the breach includes social security numbers, businesses must also offer two full years of free identity theft protection. Finally, in addition to the requirement to maintain

"reasonable safeguards" to protect D.C. residents' personal information, businesses would also have to contractually impose that obligation on any nonaffiliated third party with which businesses share that personal information. – *Karina Puttieva*

For more information, please contact:

- Valerie Breslin Montague at **vbmontague@nixonpeabody.com** or 312-977-4485
- Karina Puttieva at **kputtieva@nixonpeabody.com** or 213-629-6091

NP PRIVACY PARTNER BLOG

Staying ahead in a data-driven world: insights from our Data Privacy & Security team