November 9, 2018

What's trending on NP Privacy Partner

The FCC warns robocallers, Senator Wyden (D-OR) introduces draft data privacy bill creating a national "Do-Not-Track" system and more. Here's what's trending in data privacy and cybersecurity.

Consumer Privacy

FCC urges robocallers to adopt call authentication system

The Federal Communications Commission (FCC) has warned robocallers that they have a year to clean up their acts, or the FCC will take action. Specifically, the FCC is pushing the implementation of a "traceback" system developed by a working group of internet engineers and other industry stakeholders that will make it easier to track the origin of calls. The FCC intends that the system will prevent robocalls from lying about the number they are calling from, making it easier to track the origin of the call.

Several industry members have already adopted the system, known as SHAKEN/STIR. The system requires telephone service providers to provide digital certificates for each telephone number issued. The digital certificates are then used by the telephone provider receiving a phone call to determine whether the incoming number is authentic or if it has been spoofed.

The FCC's push for call authentication is part of its renewed effort to rein in robocallers. "We need call authentication to become a reality—it's the best way to ensure that consumers can answer their phones with confidence," Ajit Pai, chairman of the FCC, said in a statement. Although the FCC has threatened to take action if those industry members who have not yet adopted the call authentication system do not do so within the next year, it has not said how it will go about obtaining their compliance. – *Eric M. Ferrante*

Senator Wyden (D-OR) introduces draft data privacy bill creating a national Do-Not-Track system

Last week, Senator Ron Wyden of Oregon introduced draft legislation tentatively named the Consumer Data Privacy Act. The bill gives consumers the right to opt out of systems that share their data with third parties. Specifically, it calls for the creation of a national "Do Not Track" system to stop companies from tracking internet users by sharing or selling data and targeting advertisements based on their personal information. Under this system a consumer can prevent

"covered entities from sharing the personal information of the consumer with third parties," unless the data sharing "is necessary for the primary purpose for which the consumer provided the personal information."

Where a company's free service requires a consumer to opt out of privacy protections, the company would have to give customers "an option to pay a fee to use a substantially similar service that is not conditioned upon" giving up one's privacy. In other words: sites would be allowed to charge for a version of their product that does not rely on user data to generate revenue. Moreover, the bill is limited to companies that earn more than $50 million in average annual revenue or collect personal information on at least one (1) million consumers or at least one (1) million consumer devices.

On a regulatory level, the bill would give the Federal Trade Commission (FTC) more staff and the power to write privacy regulations. And, the FTC would be able to fine companies for a first offense. Echoing the EU General Data Protection Regulation (GDPR), the bill sets maximum fines at four (4) percent of the revenue. Most controversially, in addition to fines of up to $5 million, senior executives who violate privacy and cybersecurity standards and knowingly mislead regulators could face up to 20 years in prison.

Notably, the bill doesn't currently say whether the federal government should preempt state rules or address the ability of citizens to sue in certain privacy cases.

Given the drastic penalties, the bill is unlikely to pass in its current form. But, given the mixed industry reaction to California's far-reaching Consumer Privacy Act of 2018, set to go into effect on January 1, 2020, this likely won't be the last attempt at a federal data privacy law that we see between now and 2020. – *Karina Puttieva*

Health Care and HIPAA

Updated tool assists HIPAA covered entities and business associates complete mandatory security risk analysis

The HIPAA Security Rule has long required covered entities and business associates to conduct an enterprise-wide security risk analysis. This analysis must assess the potential risks and vulnerabilities to the confidentiality, availability and integrity of electronic protected health information ("ePHI") held by the entity. This analysis should, in part, identify where entity holds ePHI, how it receives ePHI and what the threats are to the entity's information systems that contain ePHI.

While there is no single method of conducting a risk analysis that equates to compliance with the HIPAA Security Rule, the Department of Health and Human Services (HHS), Office for Civil Rights (OCR) and the HHS Office of the National Coordinator for Health Information Technology (ONC) developed a Security Risk Assessment Tool (the "SRA Tool") to assist covered entities and business associates in completing this required task. OCR and ONC state that the SRA tool is designed to be used by small or medium-sized health care practices or other covered entities and business associates, but its concepts can be applied to covered entities and business associates of all sizes.

In October 2018, OCR and ONC announced changes to the SRA Tool to make it more user-friendly and more broadly applicable. The updated version follows comprehensive testing of the prior model with health care practice managers. One major update is enhanced ways for an entity to document how it can implement or plan for security measures to protect its ePHI. It also includes new

features, such as a progress tracker, a method of tracking business associates and assets and improvements to ratings of threats and vulnerabilities.

The updated SRA Tool is one more way in which OCR indicates the importance of conducting security risk analyses. Failure to conduct such an analysis can put an entity's ePHI at a higher risk, and can be a major factor weighing in favor of penalties or other enforcement if OCR audits or investigates a covered entity or business associate. Many of the OCR enforcement actions over the past several years reference lack of a security risk analysis as part of the identified compliance issues (see our prior summaries here, here, and here).

The updated SRA Tool can be found here. OCR and ONC note that the update is compatible with Windows operating systems only; iPad users can continue to use the prior version. – *Valerie Breslin Montague*

For more information, please contact:

- Eric M. Ferrante at **eferrante@nixonpeabody.com** or 585-263-1362
- Karina Puttieva at **kputtieva@nixonpeabody.com** or 213-629-6091
- Valerie Breslin Montague at **vbmontague@nixonpeabody.com** or 312-977-4485

NP PRIVACY PARTNER BLOG

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