NOW + NEXT

NP PRIVACY PARTNER | NIXON PEABODY LLP

JUNE 9, 2017

What's trending on NP Privacy Partner

Supreme court to review permissibility of cell phone data collection, a task force identifies six high-level imperatives to improve the health care industry's cybersecurity, a recap of the Society on Corporate Compliance and Ethics podcast and a house bill could create new online privacy rules under FTC jurisdiction. Here's what's trending in data privacy and cybersecurity.

Consumer Privacy

Supreme Court to review permissibility of cell phone data collection

The Supreme Court of the United States agreed to hear a case that considers whether the Fourth Amendment requires warrants for search and seizures of historical cellphone records that would reveal the location and movements of a user. The case, *Carpenter v. US*, affirmed by the Sixth Circuit in April 2016, found that a warrant was not required under the Fourth Amendment for cell phone location data because it did not reveal anything about the actual content of the communication. Therefore, the data was instead a routinely collected business record and there was no reasonable expectation of privacy.

In April 2011, using data obtained from various cell phone signal towers, police arrested Timothy Carpenter and Michael Sanders who were suspected of committing numerous armed robberies in the Detroit area. The FBI was able to create a map allegedly showing where Carpenter and Sanders had used their cell phones on the days of the robberies. The map showed the men within a half mile to a two-mile vicinity.

The government obtained the data pursuant to a court order issued under the Stored Communications Act ("SCA"). After hearing this data, as well as testimony from seven accomplices, a federal jury convicted both men in 2013. Carpenter received a 116-year prison sentence. Sanders received 14 years.

On appeal to the Sixth Circuit, the defendants in *Carpenter* argued that the Fourth Amendment required the government to meet the higher-standard of probable cause rather than the relevance and materiality required by the SCA. For over twenty years, the SCA has authorized investigators to obtain cell-site data on a showing of reasonableness. The defendants further argued that cell phone location data reveals private details of one's life and is a new form of electronic surveillance. The Sixth Circuit disagreed.

In taking the case, the Supreme Court has the opportunity to set a standard for locational privacy that could have far-reaching effects in both law enforcement investigations and the online industry. – *Jenny L. Holmes*

Health Care / HIPAA

Task force warns of the critical condition of health care industry cybersecurity

On June 2, the Health Care Industry Cybersecurity Task Force submitted to Congress its Report on Improving Cybersecurity in the Health Care Industry, with warnings about the growing challenges of intentional and unintentional cyber incidents with our nation's health care. The Task Force, a public-private partnership created by the Cybersecurity Act of 2015, stressed that "[n]ow more than ever, all health care delivery organizations … have a greater responsibility to secure their systems, medical devices, and patient data."

As noted by the Task Force, the United States health care industry is a "mosaic," including large health systems, single physician practices, public and private research payers, research institutions, medical device developers and software companies, and a diverse patient population. This mosaic creates challenges to uniformity in cybersecurity and barriers to improvements. Further, a "matrix of well-intentioned federal and state laws and regulations" must be understood, implemented and coordinated.

Too often, health care administrators and practitioners assume that their IT networks and devices are functioning without cybersecurity vulnerability and that their IT departments are the only focal points to address cyber concerns. Such passivity can have dangerous and drastic implications, as recent ransomware incidents have demonstrated that health care delivery organizations can be interrupted due to a system compromise.

The Task Force identified the following six high-level imperatives by which to organize its recommendations and action items to improve the health care industry's cybersecurity:

1. Define and streamline leadership, governance and expectations for cybersecurity
2. Increase security and resilience of medical devices and health IT
3. Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities
4. Increase health care industry readiness through improved cybersecurity awareness and education
5. Identify mechanisms to protect research and development efforts and intellectual property from attacks and exposure
6. Improve information sharing of industry threats, weaknesses and mitigations

The recommendations include action items for implementation and identify key players to ensure their success. Most of all, the government and private health care sector must ensure that there are adequate resources and national collaboration in the face of ever-evolving cyber threats, which often specifically target the vulnerabilities of the health care industry due to the immediate impacts that disruptions can cause. – *Steven M. Richard*

Podcast highlights OCR enforcement trends and future rulemaking

This post originally appeared on American Health Lawyers Association on June 1, 2017.

On May 15, 2017, the Society on Corporate Compliance and Ethics posted a podcast of an interview with Iliana Peters, Senior Advisor for HIPAA Compliance and Enforcement at the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR). In the podcast, Ms. Peters discusses OCR enforcement trends, upcoming rulemaking, and the National Institutes of Health's (NIH's) All of Us Research Program (All of Us Program).

Ms. Peters discussed the different ways that compliance issues come to the attention of OCR, such as through complaints, breaches, from the media, or from other federal or state agencies, and how OCR sees the same types of compliance issues repeated again and again. She provided some insight as to how OCR chooses which cases to pursue, stating that OCR tends to pick cases with particularly egregious violations or those that will "send a message to the industry and be a teachable moment" to highlight OCR's enforcement concerns. Examples of enforcement trends that are found in many recent OCR settlements include the lack of an enterprise-wide risk analysis, disclosures to third parties without HIPAA-compliant authorizations, and security issues related to portable media, such as laptops, thumb drives, phones, and other devices.

The podcast also addressed cybersecurity issues. In particular, Ms. Peters addressed the widespread issues related to ransomware, stating her view that ransomware will lead to a reportable breach in the "majority" of cases. She stated that OCR will expect an organization to provide support as to why it determined that its data was not compromised if it concludes a ransomware attack is not a reportable breach of unsecured protected health information.

In addition to addressing enforcement issues, Ms. Peters discussed OCR's current rulemaking efforts, describing how the agency is working on a Notice of Proposed Rulemaking (NPRM) on the Health Information Technology for Economic and Clinical Health (HITECH) Act provision that will permit individuals harmed by HIPAA violations to share in the penalties related to such violations. Ms. Peters described the difficulty in crafting rules that attempt to quantify harm and that establish a formula for dividing a penalty or other recovery. She stated that OCR is still working on this NPRM.

Ms. Peters also described how OCR is continuing to work on rules governing the accounting of disclosures that is required under the HIPAA Privacy Rule. She stated that the previous NPRM on this issue resulted in numerous comments describing the burdens that would result from the HITECH Act's requirements and that OCR is working to determine the appropriate way to implement the HITECH Act requirements while simultaneously addressing the public's concerns.

Finally, the podcast conversation addressed the NIH's All of Us Program, which is attempting to work with over a million individuals. NIH wants to collect health information from these individuals and analyze for long-term trends to understand general health risks to our society and to further enable precision medicine. Ms. Peters stated that OCR is working closely with those implementing the All of Us Program to ensure that privacy and security protections are in place even though the All of Us Program is not regulated by HIPAA.

Access the podcast. – *Valerie Breslin Montague*

Cybersecurity

House bill would create new online privacy rules under FTC jurisdiction

After leading the charge to repeal the Federal Communications Commission's (FCC) online privacy rules, U.S. Rep. Marsha Blackburn (R-Tenn.) has introduced the Balancing the Rights of Web Surfers Equally and Responsibly Act (the "Browser Act"), a bill that would require internet service providers and online companies to receive opt-in or opt-out options for sharing "sensitive user information" while establishing the Federal Trade Commission (FTC) as the sole online privacy regulatory. According to Blackburn, who chairs the House Energy and Commerce Subcommittee on Communications and Technology, the FCC's rules "created confusion by establishing two privacy regulators" and the Browser Act would create "a level and fair privacy playing field by bringing all entities that collect and sell the personal data of individuals under the same rules."

According to language in the bill, the Browser Act would "require providers of broadband internet access service and edge services . . . to give users opt-in or opt-out approval rights with respect to the use of, disclosure of[] and access to user information collected by such providers based on the level of sensitivity of such information, and for other purposes[.]" This approach would require the FTC, which would be vested with exclusive regulatory jurisdiction over online privacy, to adopt the FCC's now-repealed opt-in approach to customer consent. But, according to some experts, the bill would take those rules further than they went before. This is because the bill would apply to both internet service providers and so-called "edge providers" like Google and Facebook. Edge providers were not covered by the FCC's previous rules.

There remains uncertainty about the implementation of the rules should the Browser Act pass in the House and Senate, however. Although the text of the bill says it applies to broadband providers, they are largely exempt from FTC jurisdiction as common carriers under Title II of the Communications Act, a classification established under the FCC's 2015 Open Internet Order. If the FTC's new acting chairman, Maureen Ohlhausen, gets her way and the Open Internet Order is undone, the problems of implementation may be avoided. –E*ric M. Ferrante*

For more information, please contact:

— Eric M. Ferrante at **eferrante@nixonpeabody.com** or 585-263-1362
— Jenny L. Holmes at **jholmes@nixonpeabody.com** or 585-263-1494
— Valerie Breslin Montague at **vbmontague@nixonpeabody.com** or 312-977-4485
— Steven M. Richard at **srichard@nixonpeabody.com** or 401-454-1020