OCTOBER 28, 2016

What's trending on NP Privacy Partner

A cybersecurity conference aims to find the balance between security and privacy; New York proposes strict regulations on financial institutions; Spokeo provides insight on standing for FCRA claims; HHS issues cooperative agreements to streamline cyber threat information sharing; New HIPAA settlement emphasizes importance of a "living" security risk assessment; and Journalist wins years-long FOIA fight against federal government.

Cybersecurity

The University of Michigan hosts cyber security conference

This past Thursday, October 20, 2016, The University of Michigan in Ann Arbor held its 12th annual conference, SUMIT 2016, on cyber security at Michigan's Rackham Auditorium. Michigan welcomed industry leaders to speak at this event, one being Donald Welch. Immersed in the field as Michigan's Chief Information Security Officer, Mr. Welch spoke at the event and highlighted the interplay between privacy and cyber security. Essentially, increasing security is going to decrease privacy for the average American. Striking this balance is something that always invites challenging discussion for various legislative bodies and courts around the country, including the Supreme Court of the United States.

The arena of cyber security is vast, affecting many other worldwide phenomena and societal systems including terrorism, social media, airport security, health care, the criminal justice system (particularly criminal procedure) and daily activities, such as one using apps on his or her smart phone. In an age where there can be more personal information stored on your mobile device than in your entire house, privacy is more important than ever. Health care attorneys and medical professionals alike should be closely monitoring how the health care privacy laws evolve and possibly become more robust as we get deeper into the 21st century.

In a century where technology seems to be driving our advancement, cyber security will become a saturated field with universities such as Michigan pulling their resources together to resolve current issues and also take the lead in forward thinking.—Kristen Marotta

New York proposes strict cybersecurity regulations on financial institutions and insurers

On September 13, the New York Department of Financial Services (DFS) proposed demanding cybersecurity regulations for financial institutions and insurers. The proposed regulations incorporate ideas from federal regulations like the Securities and Exchange Commission's Regulation Systems Compliance and Integrity as well as move toward European Laws. Most major financial institutions and insurers already have similar measures in place.

The proposed regulations require all state-regulated banks and insurers to annually assess their cyber vulnerabilities as well as develop data and system protection policies and immediate security breach response plans. Each entity would have to designate a chief information security officer (CISO) who is responsible for biannually submitting a report to the board of directors on the effectiveness of the cybersecurity policy.

The regulations would require companies to have thorough written cybersecurity policies that a board of directors must review and a senior office must sign off on. Entities would be required to annually submit to the DFS a certification of compliance and would have 72 hours to notify DFS of "any material risk of imminent harm relating to its cybersecurity program."

If enacted, the regulations could have immediate and long-term implications in and out of New York. Similar to the recently enacted Privacy Shield between the European Union and the U.S., Section 500.11 of the DFS proposal requires that any contracted third-party vendors with access to the covered entities' information systems or non-public information utilize similarly stringent cybersecurity policies. This necessarily brings data protection to the forefront of contract negotiations between covered entities and their service providers and, as a result, could have the effect of promoting strong cybersecurity across various industries.

However, the regulations could have serious cost and resource effects on smaller and midsized companies. Compliance—especially if entities do not already have a cybersecurity routine in place—will likely prove to be a challenge.

A 45-day public comment period began September 28, 2016. The proposed regulations will take effect on January 1, 2017. Covered entities will have 180 days to comply. The full text of the proposed regulations can be found here.—Jenny R. Lewis

Enforcement Litigation

Spokeo providing a successful basis for challenging plaintiffs' standing in no-harm FCRA cases.

Although the Supreme Court's May 16, 2016, decision in *Spokeo, Inc. v. Robins* did not decide the case before it, *Spokeo* has recently been applied by a number of federal district courts to dismiss Fair Credit Reporting Act (FCRA) cases in which the plaintiffs failed to show they suffered concrete harm.

In the past few weeks, courts have held that alleged failures to provide proper notice or other similar procedural or technical violations, standing alone, are not sufficient to maintain Article III standing to sue in federal court. Among the recent cases finding a lack of standing are *Nokchan v.*

Lyft, Inc., 2016 U.S. Dist. LEXIS 138582 (N.D. Cal. Oct. 5, 2016); *Baker v. Microbilt Corp.*, 2016 U.S. Dist. LEXIS 137946 (M.D. Pa. Oct. 3, 2016); *Frankenfield v. MicroBilt Corp.*, No. 4:14-CV-1112, 2016 U.S. Dist. LEXIS 137944 (M.D. Pa. Oct. 3, 2016); *Salvatore v. Microbilt Corp.*, No. 4:14-CV-1848, 2016 U.S. Dist. LEXIS 137943 (M.D. Pa. Oct. 3, 2016); *Owner-Operator Indep. Drivers Ass'n, Inc. v. United States DOT*, 2016 U.S. Dist. LEXIS 135630 (D.D.C. Sept. 30, 2016); and *Disalvo v. Intellicorp Records, Inc.*, 2016 U.S. Dist. LEXIS 133344 (N.D. Ohio Sep. 27, 2016).

These courts have noted that where plaintiffs cannot show that the alleged FCRA violations resulted in the loss of a job opportunity or the unlawful disclosure of private information, for example, they cannot show the "concrete harm" *Spokeo* requires to maintain standing. On the whole, these recent decisions do not seem to be receptive to arguments that technical FCRA violations *ipso facto* cause concrete harm based on theories of invasion of privacy or "informational injury"; instead, they read *Spokeo* to require some real-life harm beyond the violation of the statute itself. Decisions like these should significantly limit—if not eliminate—the viability of harm-free FCRA suits seeking only statutory damages, including putative class actions, in federal court.—Matthew J. Frankel

Health Care and HIPAA

HHS issues cooperative agreements in hopes of streamlining cyber threat information sharing.

Earlier this month, the U.S. Department of Health and Human Services (HHS) awarded cooperative agreements totaling $350,000, as part of a continuing effort to provide the health care and public health sector with tools to identify and respond to cybersecurity threats.

Both cooperative agreements were awarded to the National Health Information Sharing Analysis Center (NH-ISAC) of Ormond Beach, Florida. The purpose of the first cooperative agreement, issued by HHS's Office of the National Coordinator for Health Information Technology, is to provide cybersecurity information and education on cyber threats to health care sector stakeholders. HSS's Office of the Assistant Secretary of Preparedness and Response awarded the second cooperative agreement to NH-ISAC to help build the infrastructure necessary to disseminate cyber threat information securely to health care partners.

The result will be a streamlined cyber threat information sharing process whereby HHS will be able to send information to a single entity, which in turn will share this information widely with other health care organizations. This system is particularly beneficial for smaller health care providers that otherwise might not have the resources to enlist the help of information sharing and analysis organizations.

The full HHS press release can be accessed here.—Michal E. Ovadia

New HIPAA settlement emphasizes importance of a "living" security risk assessment.

On October 18, 2016, the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) released details of a $2.14 million settlement and corrective action plan with St. Joseph Health, a nonprofit, multi-facility health system serving California, Texas and New Mexico (SJH).

In February 2012, SJH reported a breach involving 31,800 patient files that were publicly accessible on the internet for a period of over one year. SJH purchased a new server and the file sharing application on the server had a default setting that allowed for public access. The information that was publicly accessible included names, diagnoses and demographic information, among other information, but did not include social security numbers or financial information.

A key finding from OCR's investigation relates to the HIPAA requirement for covered entities and business associates to conduct a security risk assessment. OCR found that the new server created an "environmental or operational" change, which required a review of, or update to, SJH's security risk assessment. OCR states that SJH compromised the security of its electronic protected health information because it did not perform an evaluation in response to the addition of the new server. Notably, after the discovery of the breach to the present, OCR found that SJH "failed to satisfactorily conduct an accurate and thorough analysis of the potential risks and vulnerabilities" to its electronic protected health information. This provides a key take away to covered entities and business associates that changes in processes, equipment, software and similar items necessitate a review and potentially an update of the entity's security risk assessment.

SJH's settlement with OCR follows a $15 million class action lawsuit settlement, pursuant to which SJH agreed to pay $7.5 million to the 31,800 impacted patients and the remaining $7.5 million for attorneys' fees and legal costs. The class action settlement also required SJH to establish a $3 million fund, permitting patients who could demonstrate that they suffered losses to apply for up to $25,000 each.

As evidenced by the time lapse between this breach and the settlement, it seems as though OCR is continuing to work its way through its enforcement of breaches reported over the last several years.

The SJH Resolution Agreement and Corrective Action Plan can be found here.—Valerie Breslin Montague

Privacy Litigation & Class Action

Journalist wins years-long FOIA fight against federal government.

Last month, the United States District Court for the District of Rhode Island granted a local journalist's request that the federal government be required to hand over requested trial exhibits of a high-profile criminal trial. Philip Eil, a journalist based in Providence, Rhode Island, had been chasing these exhibits since the conclusion of the criminal trial in 2011. (Mr. Eil has not yet received the records—the court provided the government sixty (60) days to release the exhibits.) After multiple avenues were closed to him, including filing a Freedom of Information Act ("FOIA") request, he filed a lawsuit in federal court in Rhode Island seeking these exhibits. (Nixon Peabody, LLP attorneys Neal J. McNamara and Jessica Schachter Jewell, along with the American Civil Liberties Union of Rhode Island, represented Mr. Eil in this matter.)

For Mr. Eil, his request for the records has always been simple: he should be able to see what the jury saw and therefore what the government used to prosecute and convict a physician to four consecutive sentences in prison. Despite his seemingly simple request, the United States Drug Enforcement Agency ("DEA") withheld a large majority of the exhibits (and also provided largely redacted and essentially meaningless records), citing privacy concerns in response to Mr. Eil's FOIA

request. Because the victims were patients of the physician who was tried, a vast majority of the trial exhibits were their medical records, which clearly contained private information that otherwise would never have been public records. But they were made public when the government chose those documents to support its high-profile prosecution.

This tension—the right to public trials on the one hand and an individual's right to privacy on the other, especially with respect to something normally so private as their medical information—was front and center at the summary judgment hearing before Judge John J. McConnell, Jr. earlier this summer. Despite the legitimate concerns on both sides, Judge McConnell asked the government how it could refuse to release the trial exhibits after the government had introduced them as part of a public trial (and failed to take any measures to protect the information in that venue).Ultimately, Judge McConnell noted the "societal benefits" of public scrutiny of judicial proceedings and commented on the "tenacious journalists" who have exposed potential flaws in criminal cases over the years, citing to the popular National Public Radio podcast *Serial* and Netflix's *Making a Murderer*. Weighing the private and public interests, Judge McConnell held that "[b]ecause the information petitioned for disclosure is the very information used to convict [the physician], the public interest in this information cannot be served in any way other than by releasing the court exhibits. Indeed, these particular documents are an integral part of a serious investigation and prosecution by the DEA[.]" The decision noted that certain, limited information could be redacted and that the government should renumber the exhibits, so as to limit intrusion into these individuals' privacy (e.g., so as to avoid matching up the records to the exhibit list and/or transcript, which named these individuals by name).

The government still has time to appeal. But, for now, this ruling has squarely come down on the side of the right to public information.—Jessica S. Jewell

For more information, please contact:

— Matthew J. Frankel at **mfrankel@nixonpeabody.com** or 617-345-1038
— Jessica S. Jewell at **jjewell@nixonpeabody.com** or 401-454-1046
— Jenny R. Lewis at **jlewis@nixonpeabody.com** or 585-263-1494
— Kristen Marotta at **kmarotta@nixonpeabody.com** or 516-832-7513
— Valerie Breslin Montague at **vbmontague@nixonpeabody.com** or 312-977-4485
— Michal E. Ovadia at **movadia@nixonpeabody.com** or 516-832-7634

NP PRIVACY PARTNER BLOG

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