JANUARY 12, 2018

What's trending on NP Privacy Partner

Don't rush to implement fixes for Meltdown and Spectre, court weighs the victim-advocate privilege in Title IX lawsuits, FTC paper addresses security issues related to connected cars, and more. Here's what's trending in data privacy and cybersecurity.

Cybersecurity

Don't rush to implement fixes for Meltdown and Spectre

Meltdown and Spectre are critical security vulnerabilities in modern processors. These hardware bugs allow programs to steal data currently processed on the computer. However, rushing to "plug the holes" of these vulnerabilities will certainly lead to bigger problems for an organization.

On January 3, 2018, the hardware bugs dubbed Meltdown and Spectre were discovered by researchers. Meltdown and Spectre are critical security vulnerabilities in modern processors. These hardware bugs allow programs to steal data currently processed on the computer. While programs are typically not permitted to read data from other programs, a malicious program could exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs. This might include your passwords stored in a password manager or browser, your personal photos, emails, instant messages and even business-critical documents.

There are three main types of companies responding to Meltdown and Spectre: processor companies (Intel and AMD), operating system companies (Microsoft, Google, Apple) and cloud providers (Microsoft/Azure, Amazon).

Recommendations for "fixing" this vulnerability have been varied and, in my opinion, incomplete and "too soon" to implement. Many companies have issued advisories about the flaws. For example, Intel plans to have software and firmware updates available by January 12 to address the Spectre and Meltdown vulnerabilities in 90% of the affected processors sold since 2013. The flaws affect all processors sold over the past twenty years. Intel says that fixes for older processors will be available in the future. Microsoft issued patches for its supported operating systems. However, there have been reports that after the patches have been applied, there have been significant performance issues—as high as a 50% degradation in CPU performance on some of the newest CPUs. Also, certain antivirus products no longer work or crash the system after the patches are applied. Due to the uncertainty of what patching and/or hardware fixes will do to your device, remember these vulnerabilities affect almost every device that uses a CPU (routers, firewalls, switches, tablets,

This newsletter is intended as an information source for the clients and friends of Nixon Peabody LLP. The content should not be construed as legal advice, and readers should not act upon information in the publication without professional counsel. This material may be considered advertising under certain rules of professional conduct. Copyright © 2017 Nixon Peabody LLP. All rights reserved.

etc.). I would not apply any patch or hardware fix upon first release. As the saying goes, the cure may be worse than the disease (at least for now).

In my opinion, more research and testing needs to be done by researchers, the IT community and internal information technology organizations. Your IT departments need time to assess your environment, work with your company's various hardware and software vendors, test patches and hardware fixes and develop a game plan for company-wide implementation with minimal disruption to your business.

No one should make the mistake of believing that the targeted vulnerabilities will be fixed in a short period of time. Rushing to "plug the holes" of these vulnerabilities will certainly lead to bigger problems for an organization. As of this post, not a single piece of malicious code that exploits these vulnerabilities has been reported to have been released. This an important fact given these vulnerabilities have been in existence for the past twenty years. Contrarily, now that these vulnerabilities have been disclosed, I would suspect there will be a rash of exploits delivered if not within days, certainly weeks. – *John G. Roman, Jr., CISSP*

Privacy Litigation

Title IX lawsuit weighs the victim-advocate privilege

Court continue to weigh privacy interests in Title IX lawsuits, particularly relating to privileges and confidentiality in discovery.

A federal judge in the Eastern District of Virginia recently ruled that conversations between an alleged sexual assault victim and her advocate are not protected in the same way as attorney-client or doctor-patient communications. In Jane Doe v. Old Dominion University, Plaintiff Jane Doe ("Doe"), a student at Old Dominion University ("ODU"), sued the university under Title IX relating to her alleged sexual assault.

As part of discovery in the litigation, ODU served a subpoena *duces tecum* on SurvJustice, a victim advocacy legal group, for messages between Doe and her parents and SurvJustice before Doe became its legal client. SurvJustice refused claiming the prior communications were protected by the "victim-advocate privilege" allegedly created by Va. Code Ann. § 63.2-104.1.

ODU filed a motion to compel Doe (and her parents) and SurvJustice to provide the requested documents. ODU argued that the privilege did not apply, that Doe had already provided communications with a prior victim advocate, and that any produced documents would be under seal to protect Doe's anonymity. Doe's counsel countered that production would unduly invade the necessity of a confidential relationship between a sexual assault victim and an advocate.

The Court found that "there exists a limited victim-advocate privilege which applies to the withheld email and other communications between Plaintiff and her parents and her victim advocate SurvJustice." The Court noted that thirty-nine states, including Virginia, have adopted laws protecting some level of confidentiality for victim-advocate communications. The Court continued, "[h]owever, such privilege is not absolute" and ordered Doe and SurvJustice (and Doe's parents) to produce the withheld documents for an in camera inspection to determine whether any are relevant to any of ODU's defenses. One example the Court provided was any communication that may relate to issues of consent underlying the incident. From the Court's order, it appears that the SurvJustice documents may include the Plaintiff's cellular phone records.

Through its in-camera review, the Court determined that some of the documents, described as "emails," are "subject to production." Because the Court ordered these documents produced under seal, it is not possible to determine the full nature and scope of the records the Court ordered produced.

We will continue to follow similar developments in the evolving area of Title IX litigation, particularly as courts address vexing issues of privileges and privacy that require the balancing of competing considerations. – *Kevin Saunders*

Healthcare and HIPPA

SAMHSA issues final rule implementing changes to Confidentiality of Substance Use Disorder Patient Records regulations

SAMHSA issues new rule with stricter privacy safeguards to protect individuals with substance use disorders from discrimination and misuse of records.

Our latest Health Care Alert analyzes The Substance Abuse and Mental Health Services Administration's recent final rule (the "Rule") implementing changes to the Confidentiality of Substance Use Disorder Patient Records regulations at 42 C.F.R. Part 2. The new Rule further amends the Part 2 regulations that were the subject of significant rulemaking published in January 2017. This Rule may not end SAMHSA's efforts to align Part 2 more closely with HIPAA. Our Alert on this important regulatory development may be viewed here. – *Laurie Cohen, Jena Grady, Valerie Breslin Montague*

Consumer Privacy

FTC paper addresses security issues related to connected cars

Connected vehicles offer consumer benefits with privacy risks.

The Federal Trade Commission's Bureau of Consumer Protection has issued a paper summarizing key takeaways from its June 28, 2017, workshop co-hosted with the National Highway Traffic Safety Administration, which focused on privacy and security issues related to connected cars. The FTC provides the following summary of the benefits and risk of the expanding technology:

"Modern motor vehicles increasingly are equipped with technologies that enable them to access information via the Internet and gather, store, and transmit data for entertainment, performance, and safety purposes. Automated vehicles, those with vehicle-to-vehicle (V2V) communications technology, and other forms of wireless connectivity can provide important benefits to consumers and have the potential to revolutionize motor vehicle safety. At the same time, these technologies raise privacy and security concerns."

As one of the key points of the emerging technology, many companies throughout the connected car ecosystem collect data that is often used to enhance consumer benefits. Data may be collected for service purposes, particularly relating to driver habits. Insurance companies may use the data to provide discounts based upon demonstrated good driving habits.

The types of data collected through connected cars range from non-sensitive data about the vehicle to individualized personal data. Non-sensitive data can include aggregate information used for traffic management purposes to reduce congestion. Vehicles may collect information about occupants themselves, including fingerprints and iris pattern used for authentication purposes.

All of this data collection leads to concerns about secondary, unexpected uses, which could be sold to third-parties that may use the information to target consumers. Notice and disclosures are key topics as the collection, usage and sale of the accumulated data become more prevalent.

Also, connected and autonomous cars will have cybersecurity risks, which could allow a hacker to impair or take control of vehicle functions. Panelists at the FTC workshop stressed the importance of information sharing among manufacturers and associations within the automotive industry. In network design, safety critical functions should be segregated from other connected functions. Of particular importance, the panelists stressed the importance of industry self-regulation in adopting security best practices, using governmental standards such as the NIST framework as a baseline.

The connected car marketplace will only expand, which offers both efficiencies and risks to consumers. Education of consumers will be vital as industry stakeholders work to ensure the protection of compiled information. – *Steven M. Richard*

For more information, please contact:

- John G. Roman, Jr. at **jroman@nixonpeabody.com** or 585-263-1378
- Kevin Saunders at **ksaunders@nixonpeabody.com** or 585-263-1561
- Laurie Cohen at **lauriecohen@nixonpeabody.com** or 518-427-2708
- Jena Grady at **jgrady@nixonpeabody.com** or 212-940-3114
- Valerie Breslin Montague at **vbmontague@nixonpeabody.com** or 312-977-4485
- Steven M. Richard at **srichard@nixonpeabody.com** or 401-454-1020

NP PRIVACY PARTNER BLOG

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