SHARE:

Join Our Email List

View as Webpage

July 6, 2022

Welcome

Welcome to the 13th issue of *Decoded* for the year.

Did you know that we have a practice group devoted to Cybersecurity & Data Protection? Our cybersecurity team is drawn from a variety of practice groups to provide a holistic approach to working with your organization to protect its data. Our lawyers know your industry, and we partner with our clients to create a data security plan tailored to your organization's specific needs and situation. Our cybersecurity team has advised organizations across industry sectors, including clients in the healthcare, financial, and education industries, on how to navigate the ever-changing cybersecurity environment. We work with clients to address a broad range of issues related to cybersecurity incidents and have been called upon to assist with every phase of data breach management, from preparedness and prevention to mitigation and resolution. This ranges from advising clients on employee training on cybersecurity, responding to a lost device that contains sensitive data, responding to a compromising data breach, and defending against government inquiries and civil litigation resulting from a cyberattack.

Please feel free to reach out if you have specific questions about this area of the law - or any area where your company may need guidance. Click here to learn more about this specific practice.

We hope you enjoy this issue and, as always, thank you for reading.

Nicholas P. Mooney II, Co-Editor of *Decoded,* Chair of Spilman's Technology Practice Group, and Co-Chair of the Cybersecurity & Data Protection Practice Group

and

Alexander L. Turner, Co-Editor of *Decoded* and Co-Chair of the Cybersecurity & Data Protection Practice Group

AHA Expresses Member Support for PATCH Act, Medical Device Security

"In a letter addressed to Senators Bill Cassidy (R-LA) and Tammy Baldwin (D-WI), who first introduced the PATCH Act, the AHA said that the association and its members were committed to preventing cyberattacks and would support the PATCH Act's intentions of doing the same via medical device security improvements."

Why this is important: The American Hospital Association ("AHA") has announced its support of the PATCH Act, introduced this year as bicameral legislation aimed at enhancing cybersecurity of medical devices. The AHA consists of approximately 5,000 member healthcare organizations nationwide and represents the interests of a significant portion of the overall healthcare system in the United States. This is a positive step toward advancing the legislation and shows a growing level of industry support for the PATCH Act. Importantly, the AHA has identified additional industry concerns with the current draft language of the PATCH Act. In its letter to the two supporting Senators, the AHA recommended adding a provision to the PATCH Act to clarify that continuing FDA approval of cyber devices would not be jeopardized as manufacturers implement their device updates. Because so many hospital systems rely on legacy devices and systems, it will be critical to continuity of care that those in the industry be able to rely on their devices retaining approved status, even while security updates are rolled out. Including such a provision would certainly ease liability concerns among providers and practitioners in their day-to-day operations that rely on these systems. In addition, manufacturers would benefit from the clarification that their cyber devices would not need additional approvals after each round of patches and updates. --- Brian H. Richardson

---

Data Breach Class Action Litigation and the Changing Legal Landscape

"The number and size of settlements like these are playing a role as political leaders consider new legislation regarding data privacy protection, especially when considering whether to create private rights of action."

Why this is important: Data breaches are becoming more common and more expensive. The expense of these increasing data breaches is primarily tied to the class actions that inevitably follow. These class actions can cost a company tens, if not hundreds, of millions of dollars to settle. As we have discussed in previous issues of *Decoded*, recent court rulings, like the Supreme Court's ruling in *TransUnion LLC v. Ramirez*, have tempered this risk by requiring putative class members to plead that that they have suffered an injury-in-fact in order to have standing to bring their claims. In an attempt to circumvent the Supreme Court's ruling in *TransUnion*, plaintiffs' counsel are bringing these actions in state court where the standing requirements are usually lower. In an attempt to standardize U.S. privacy laws, Congress is currently debating the American Data Privacy and Protection Act. If passed, the Act would preempt the various state privacy laws. It would also allow for a limited private cause of action. Whether this bill will succeed where others have failed has yet to be seen. We will continue to monitor developments regarding this bill and provide you with updates. --- Alexander L. Turner

---

GAO Calls on HHS to Improve Healthcare Data Breach Reporting Process

"In a new report, GAO suggested that HHS improve its healthcare data breach reporting process to allow entities to provide feedback on it."

Why this is important: The number of reported healthcare-related data breaches has increased rapidly over the past few years. HHS's Office of Civil Rights lists on its internet portal those breaches that affected more than 500 individuals. In 2015, there were 270 healthcare breaches affecting 500 or more individuals. By 2021, that number had risen to 714. Reporting an incident to OCR through its portal is only the first step in the breach reporting process. The Government Accountability Office recently called on HHS to create a mechanism for entities to provide feedback on the breach reporting process. Soliciting feedback may reduce challenges entities face when reporting breaches, improve or simplify the reporting process, and reduce lapses in communication during breach reporting investigations. HHS agreed with the recommendations and reported that it plans to add contact information to the confirmation email entities receive when reporting a breach and implement procedures for OCR to regularly review and address emails it receives. --- Nicholas P. Mooney II

Senators Call on FTC to Investigate Apple, Google's "Deceptive" Data Privacy Practices

"Senators penned a letter to the FTC urging it to investigate Apple and Google for engaging in 'unfair and deceptive' data privacy practices considering the Roe v. Wade ruling."

Why this is important: Four Senators sent a letter to the FTC requesting an investigation into Apple and Google's "unfair and deceptive" data privacy practices. The letter alleges that the tech giants were knowingly "enabling the collection and sale of hundreds of millions of mobile phone users' personal data." These identifiers have fueled the unregulated data broker market, and while this data is supposedly anonymous, it is often possible to identify a particular consumer, especially by location records. The companies allow users to opt out, but they both enable the tracking ID by default. The Senators argue that failing to warn consumers about the predictable harms that could result from using their phones with the default settings, these companies enable government and private actors to exploit advertising tracking systems for their own surveillance. The exposure to serious privacy harms is an even more urgent matter following the repeal of *Roe v. Wade*. Last month, 40 lawmakers wrote a letter to Google on this same topic, stating "we are concerned that, in a world in which abortion could be made illegal, Google's current practice of collecting and retaining extensive records of cell phone location data will allow it to become a tool for far-right extremists looking to crack down on people seeking reproductive health care." These letters highlight how the advertising-focused digital infrastructure can be weaponized against American women, and how data privacy has far-reaching consequences we never imagined. --- Alison M. Sacriponte

Lack of Clinical Evidence 'Major Gap' in Digital Health

"Most digital health companies have a low level of 'clinical robustness' as measured by their number of regulatory filings and clinical trials, according to a paper published in the Journal of Medical Internet Research."

Why this is important: In the United States, digital health continues to be a rapidly growing sector of the overall healthcare industry. Market players span a wide range from basic step-counters and wearables to fully integrated health tracking and diagnostic systems. Funding in this industry climbed from $8 billion in 2019 to $29 billion in 2021, according to data tracked by Rock Health, a venture fund tracking the industry. A group of researchers at Rock Health and Johns Hopkins University has published a cross-sectional observational analysis of the public claims and clinical robustness of 224 digital health companies with an average age of 7.7 years. The company data were pulled from Rock Health's internal venture funding database, the FDA, and the U.S. National Library of Medicine. The study looked at public claims, funding, and clinical robustness for each company. Claims were defined broadly as unique quantitative statements about product engagement, economic, or clinical outcomes made on a company's website. Clinical robustness included a calculated score based on the number of regulatory filings or clinical trials conducted by the company. The findings are staggering -- and insightful. Despite 44 percent of companies having a clinical robustness score of zero (indicating no regulatory filing or clinical trial of the digital health product), there were 1.3 public claims made on average. Even though claims and clinical robustness are both low on average, there were several companies with much higher clinical scores (10 or more). Still, there appears to be no significant correlation between public claims, clinical robustness, or funding.

These data indicate that investors are not significantly distinguishing between companies with more robust clinical support for their claims. Companies with more robust clinical support for their digital health products could potentially benefit from marketing efforts to highlight those practices. In addition, companies with lower (or nonexistent) clinical support for their claims should be cautioned against the risks of unfounded claims. As consumers turn more and more toward digital healthcare solutions, it is critical that funding and investment be driven to supporting the best outcomes, with demonstrated clinical support. --- Brian H. Richardson

How Companies Can Use Technology and Planning to Keep Employees Safe While Traveling

"Artificial intelligence can be used to gather and analyze public data sets to detect new regulations for travel, severe weather and an area's overall safety."

Why this is important: This article argues that employers have a duty to keep employees safe, which includes employees traveling for business. Business travelers need to worry about COVID-19, extreme weather, flight delays and cancellations, civil and political unrest, crime, terrorism, route changes, and other potential threats. The article argues that waiting for local news to report on these events could take 24 to 48 hours and new AI-powered analytics can bring threat notifications and other important information to employers and employees nearly instantly. Additionally, the article suggests that employers "require employees to use appropriate technology when traveling." It is unclear what might fall under the umbrella of "appropriate technology," but it may include technology that allows employers to track employees' movements while traveling. It would seem to be inherent that an employer would need to know where an employee is in order to warn her or him of potential threats. If tracking an employee's location and movements are involved, there could be a privacy issue at play here. --- Nicholas P. Mooney II

CISA Alerts Healthcare Sector to OFFIS DCMTK Cybersecurity Vulnerabilities

"Healthcare organizations using OFFIS DCMTK software should deploy updates immediately in light of recently discovered cybersecurity vulnerabilities."

Why this is important: The Cybersecurity and Infrastructure Security Agency ("CISA") discovered three cybersecurity vulnerabilities in OFFIS DCMTK. This program "consists of libraries and applications that process Digital Imaging and Communications in Medicine (DICOM) files." These files are often used in the healthcare industry for product testing and as the basis for research projects. If these files are compromised, it can lead to denial-of-service conditions, misdirect DICOM files into random directories, or allow remote code execution. CISA recommends that users of DCMTK update to version 3.6.7 or later as soon as possible to avoid being impacted by these vulnerabilities. Additionally, CISA recommends that healthcare organizations act defensively and isolate systems using DCMTK from their business networks by putting them behind a firewall. To date, there are no known exploits of these vulnerabilities. In previous issues of *Decoded* we have discussed that now these vulnerabilities are known, it is the responsibility of CISOs and company executives and board members at healthcare organizations to recognize this threat and adequately respond to protect the organization's network. Failure to recognize this warning and implement reasonable countermeasures can result in the personal liability of the CISO, company executives, and board members if a bad actor later utilizes these vulnerabilities to attack the organization. --- Alexander L. Turner

Shifting the Cybersecurity Paradigm from Severity-Focused to Risk-Centric

"Embrace cyber-risk modeling and ask security teams to pinpoint the risks that matter and prioritize remediation efforts."

Why this is important: This article makes a forcible argument that companies should not attempt to remove all cybersecurity vulnerabilities, but instead shift their focus to addressing the unique vulnerabilities they face. Vulnerabilities are increasing at an unprecedented rate, and threat actors have gotten better at taking advantage of them. If you chase two rabbits, you will not catch either one. A company trying to chase hundreds of vulnerability rabbits runs the risks of not catching all of them, or at least the most significant ones. The article argues instead companies should take a risk-based approach when prioritizing vulnerabilities and offers questions companies should consider. First, is the vulnerability the type of thing threat actors are exploiting? Second, is the company exposed to that vulnerability, or are existing security controls protecting the vulnerable asset? Third, is the vulnerable asset mission-critical? Fourth, what would be the financial impact if the vulnerable asset is compromised? This approach and these questions arm companies to deploy a better strategy to address vulnerabilities than relying exclusively on a general or common approach to prioritizing vulnerabilities. --- Nicholas P. Mooney II

Share Tweet Share

This is an attorney advertisement. Your receipt and/or use of this material does not constitute or create an attorney-client relationship between you and Spilman Thomas & Battle, PLLC or any attorney associated with the firm. This e-mail publication is distributed with the understanding that the author, publisher and distributor are not rendering legal or other professional advice on specific facts or matters and, accordingly, assume no liability whatsoever in connection with its use.
Responsible Attorney: Michael J. Basile, 800-967-8251