SHARE:

Join Our Email List

View as Webpage

August 17, 2022

Welcome

Welcome to the 16th issue of *Decoded* for the year.

As you may know, we publish a wide variety of e-newsletters. From time to time, the topics within these publications overlap each other. We have taken note of this and have begun to include content from other publications that we believe you may find of interest. For instance, today's issue includes a couple of technology-focused articles we published in our most recent educational law insights newsletter.

Given this, there may be additional Spilman publications that you would find interesting and would like to receive. We have included a comprehensive list below. If you would like to be added to the email list for any of these, simply email us your contact information and what publication to add.

- The Academic Advisor - educational law
- All Consuming - consumer finance
- Currents - energy industry
- The Dome Report - West Virginia Legislature updates
- Promissory Notes - banking and finance
- The Site Report - construction industry
- SuperVision - labor and employment law

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

CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China

"Spurred by the passage of the CHIPS and Science Act of 2022, companies have announced nearly $50 billion in additional investments in American semiconductor manufacturing, bringing total business investment to nearly $150 billion since President Biden took office."

Why this is important: This is a mere summary by the White House of the investment money provided by the new CHIPS and Science Act of 2022. This act partially underwrites development and the manufacture of new technology, particularly in IT and chip manufacturing. Its ostensible purpose is to motivate this industry to grow, driving the economy and reducing our reliance on Asia (particularly China) for these critical products. The details will come later, and that's where the rubber meets the road. Everyone remembers Solyndra getting $535 million from a similar effort in 2011 and then closing its doors shortly thereafter. The government, federal or state, is historically bad at picking winners and losers. In the past, politics affected decisions. Time will tell if this is better, or more of the same. --- Hugh B. Wellons

FDA's Former Medical Device Cybersecurity Director Says More Investment Needed in Staffing

"Long before joining the Food and Drug Administration, Kevin Fu had been alerting officials to the need for better medical device security."

Why this is important: In previous issues of *Decoded*, we have discussed the ticking time bomb that is lax cybersecurity associated with medical devices. The FDA recently issued more robust guidelines regarding medical device cybersecurity, and Congress is currently considering legislation, including the PATCH Act, to address this problem with medical device cybersecurity. The FDA's first acting director of medical device cybersecurity, Kevin Fu, recently gave an interview regarding changing cybersecurity threats, and how medical device companies need to prepare for these changing threats. He believes the key to a safe and effective medical device is appropriate cybersecurity. He went on to say that medical device manufacturers fall in a wide spectrum on how they approach cybersecurity. Some take the threat seriously and prepare accordingly, while others do not. The lack of focus on medical device cybersecurity is likely due to a shortage of properly qualified medical device cybersecurity designers. In order to properly address the need for increased medical device cybersecurity, increased investment needs to be made in training more Operational Technology Medical Device Cybersecurity Experts. Even with the increased investment in qualified designers, the FDA still lacks sufficient resources to ensure medical device cybersecurity. Without increases in the budget for cybersecurity, the FDA will have trouble handling simultaneous cybersecurity incidents in the future. Mr. Fu also discussed the significant risk of ransomware attacks on medical facilities as a result of weak medical device cybersecurity, and the fact that medical facilities need to be vigilant and flexible to compensate for the ever-changing threats these attacks present. Regarding who is responsible for protecting medical devices from cyber threats, the manufacturer or the medical facility, Mr. Fu clarified that it is a shared responsibility. Finally, regarding the importance of the PATCH Act, Mr. Fu stated that the PATCH Act is important and well drafted to address current and future cybersecurity issues associated with medical devices. To learn more about the PATCH Act, you can read our article - The PATCH Act: Protecting Medical Devices from Cyber Attacks. --- Alexander L. Turner

Crypto and the US Government are Headed for a Decisive Showdown

"A crop of lawsuits could finally settle the question of whether most digital assets are illegal securities offerings."

Why this is important: This article discusses some of the lawsuits and potential regulations that are swirling around the crypto industry to support the headline that a showdown is coming. They include: the first cryptocurrency insider trading tipping scheme; criminal charges brought by the DOJ against employees of a crypto exchange; a civil lawsuit brought by another government agency against those employees; the SEC's lawsuit against Ripple based on the allegation that its token, XRP, is an unregistered security; the SEC's investigation of a crypto exchange for allegedly listing unregistered

securities; class action lawsuits brought by private plaintiffs alleging similar claims; the SEC's position that Bitcoin is a commodity; industry requests to the SEC to create crypto-specific regulations; and two bills in Congress that would transfer the power to regulate the industry from the SEC to the Commodity Futures Trading Commission. There's no doubt that the results of these criminal prosecutions, civil lawsuits, and potential regulation have the power to dent the crypto universe. What the ultimate outcome will be hasn't yet been determined. --- Nicholas P. Mooney II

New York Becomes First State to Mandate CLE in Cybersecurity, Privacy and Data Protection

"Only two other U.S. states mandate technology training as part of a lawyer's continuing education requirement, Florida and North Carolina."

Why this is important: New York attorneys will have new mandatory continuing legal education ("CLE") requirements focusing on cybersecurity taking effect in two waves on January 1, 2023, and July 1, 2023. By focusing the updated CLE requirements on cybersecurity, privacy, and data protection, New York is leading out on addressing a major issue in the United States. Attorneys and law firm databases are viewed as high value targets for hackers and cyberattacks, largely because of the private and confidential nature of the information they hold. While Florida and North Carolina have previously implemented mandatory CLE training on technology, New York is unique in further focusing specifically on cybersecurity and ethical issues. The new requirements have also built in a mechanism for ensuring that attorneys are keeping up-to-date: the cybersecurity credits cannot be rolled over from one year to the next. Attorneys will now be required to take at least one new credit of CLE on this topic every year. A rising tide lifts all boats, as they say, and this new requirement can only benefit clients who rely on their attorneys to protect their confidential information. Many lawyers and law firms happily go above-and-beyond the minimum CLE requirements to ensure they are using the best practices in protecting their clients. It is a very positive step to see more and more states recognize the critical need for increased cybersecurity awareness in the industry. We should look forward to more states (and law firms) to follow New York's lead on this issue. --- Brian H. Richardson

Study Says Gene Editing with CRISPR/Cas9 Can Lead to Cell Toxicity and Genome Instability

"This unwanted effect is mediated by the linchpin tumor suppressor protein p53, and is determined by the DNA sequence near the editing point and various epigenetic factors in the surrounding region."

Why this is important: We've spoken about CRISPR/Cas9 before. It is a groundbreaking method to "edit" genes. Several processes are in clinical trials to treat genetic diseases that were impossible to treat before. This most recent study in Barcelona, however, raises a specter of possible problems with the entire CRISPR/Cas9 system. We will follow this and let you know as it develops. --- Hugh B. Wellons

Hospitals have Low Level of Accountability for Connected Device Breaches

"Over half of respondents in a survey of healthcare executives from cybersecurity firm Cynerio and research group Ponemon Institute reported that senior management did not require assurances that medical or internet-connected device risks were properly monitored or managed."

Why this is important: It appears that medical providers are not heeding Mr. Fu's recommendations about their responsibilities regarding cybersecurity and connected medical devices (see above). Recent research shows that medical facilities are not taking proper precautions with protecting patients' protected health information ("PHI") from cyberattacks, ransomware, and data theft resulting from breached medical devices. In previous issues of *Decoded*, we discussed the duty of senior executives having to be up-to-date on cyber threats to their organizations, and to be proactive on finding reasonable solutions to those threats. We have also discussed how if they do not take necessary steps to secure patients' PHI, they can be held personally liable in the event of a breach. However, despite the risk of being held personally liable, almost 50 percent of respondents to a recent survey stated that even though

they are taking proper security steps to secure medical data, they do not measure the effectiveness of those security procedures regarding connected medical devices. That is a problem because 88 percent of respondents stated that at least one connected device was a contributing factor to a data breach. As we have repeatedly discussed in previous issues of *Decoded*, medical devices have significant cybersecurity vulnerabilities because they use outdated or insecure software, hardware and protocols. These issues are known to the manufacturers, and many medical devices are compromised when they leave the factory. Compounding this problem is the fact that medical facilities only spend, on average, 3.4 percent of their IT budgets on medical device cybersecurity. The problem, as Mr. Fu discussed above, is that there is a conflict over who is responsible for medical device security, the manufacturers or the end users. Regardless of who is responsible, medical facilities should at least know and monitor all of their devices connected to the internet. However, 67 percent of respondents to the survey did not even take this minimal step, and do not know the total universe of connected devices in their facility. Unfortunately, it appears that the only thing that will force medical providers to make the necessary investments in medical device cybersecurity is a significant breach. The warning signs are all there. The ability to improve security is available, even if those steps are small. There is no need for medical providers to suffer through the time and cost of a substantial cyberattack in order for them to learn this important lesson. --- Alexander L. Turner

White House to Incorporate Performance Metrics into National Cybersecurity Strategy

"The Office of the National Cyber Director is working across multiple federal agencies and private sector partners to set priorities and assess effectiveness."

Why this is important: Recently, the White House Office of the National Cyber Director has begun efforts to include real-world data regarding how the U.S. responds to cyberattacks into its analysis of how well the government and private sector are "making progress toward a resilient and secure digital infrastructure." This data also will help to prioritize resource allocation and funding. The Office's hope is to reframe the discussion from a negative one (focusing on thwarting cyber adversaries) to a positive one (emphasizing the benefits that resilient cybersecurity brings). The incorporation of real-world performance metrics into the analysis is an important component to obtaining an accurate and material measure of how well the U.S. is doing, what still needs to be accomplished, and where the priorities lie. --- Nicholas P. Mooney II

Tips for Translating Cyber Risk into Board-Friendly Language

"Just because boards are more aware of the rise in cyberattacks does not mean they understand how digital technology and cybersecurity translate into business risk."

Why this is important: Diversity of experience and opinions in leadership boards is critical to any company. Blending a variety of perspectives is a key way that companies can address challenges and drive initiatives forward to successful implementation. Cybersecurity professionals are relative newcomers to the corporate board room in the form of "chief information security officers," although the role is becoming more prevalent in recent years. CISOs are reporting having difficulty in helping other members of board leadership to catch the "vision" of cybersecurity risk and need in their organizations. The answer, as it turns out, happens to be right in line with their specific area of expertise. CISOs need to effectively "hack" their fellow board members by using the same social engineering toolkit that creates risk to the company when used by bad actors. Relying on neuroscience research that highlights the power of storytelling on affecting human brain chemistry, CISOs need to build an effective narrative that makes cybersecurity risk meaningful to others in board leadership. Building that narrative requires getting to know the board leadership on a personal level, including through background research, social events, discussing priorities and individual perspectives, and then using that information to demonstrate how cybersecurity can better promote company goals and initiatives. --- Brian H. Richardson

Most Cyberattacks Come from Ransomware, Email Compromise

"Attackers are scanning for vulnerabilities in unpatched systems within 15 minutes, stressing the pace and scale of the threat."

Why this is important: Read this if you need help staying awake at night. Most cyber-intrusions are not fancy hacking, but rather an employee screw-up that allows hackers access to the system. Often, hackers do this by "phishing" a lower-level employee and then working up to someone with greater access. Companies are developing training, firewalls, etc. to counter this access. Hackers do not stand still, either, and this outlines some techniques that hackers are using to change their playbook and make their efforts more efficient. --- Hugh B. Wellons

Amazon Can't Pause Battle with Student Over Facial Recognition

"In a ruling, U.S. District Court Judge John Chun in Seattle said the student who sued the company can proceed with discovery, referring to the process of obtaining evidence from Amazon."

Why this is important: Amazon has been sued in federal court in Seattle, Washington in a putative class action related to an alleged violation of Illinois' strict Personal Information Protection Act ("PIPA"). Specifically, the representative plaintiff, an Illinois resident, alleges that Amazon violated PIPA when it allowed the online learning company Proctor U to use Rekognition facial recognition technology to verify students' identities. Rekognition is a product developed and sold by Amazon Web Services ("AWS"), and, pursuant to the AWS website, it offers pre-trained and customizable computer vision capabilities to extract information and insights from your images and videos. The plaintiff alleges that while she was a college student in Chicago, the use of this technology was required to take exams, and that she and fellow students did not give Proctor U authorization to collect and store their biometrical data. Amazon has moved to dismiss the case because, as the back-end service provider, it did not collect or possess the plaintiff's data. Amazon also seeks dismissal because it argues that PIPA does not apply to business activities engaged in outside of Illinois, and that the plaintiff has not alleged Amazon engaged in any conduct in Illinois. Notwithstanding, the District Court Judge has permitted discovery to progress pending his decision on Amazon's Motion to Dismiss because he "is not convinced that [Amazon's] motion to dismiss will prevail." The Court noted that other similar suits regarding the collection of biometrical data had been brought in this Court, and that arguments similar to Amazon's had been rejected.

Amazon is not the only organization being sued for the alleged improper use of biometrical data related to online monitoring of exams. Proctor U has also been sued in a separate action in Illinois for violations of the Illinois Biometric Information Privacy Act ("BIPA") related to unauthorized collection and storage of students' biometrical data. That case is related to online exams, including the Test of English as a Foreign Language, Graduate Record Examination, and the Law School Admission Test. Educational institutions, like the Illinois Institute of Technology and University of Illinois at Urbana-Champaign, also have been named in suits related to violations of BIPA.

Educational institutions, and the companies that provide them with educational services, need to be sure that they comply not only with FERPA, and properly protect students' educational records, but also with state privacy laws. Because the U.S. does not have a universal privacy law, educational organizations providing educational services must examine the privacy laws of each state in which they operate, because there is much variation between the states. This is especially true as remote learning continues to grow. While the educational services may be provided in a state with weaker privacy laws, the students being serviced may be located in states like California and Illinois that have strong privacy laws. The result is actions that are perfectly acceptable in one state may result in litigation in another because of where the student resides. From a practical standpoint, when developing institutional privacy policies that apply to all students, it would prudent for colleges to consider the most restrictive, consumer-friendly states' laws as their starting point. --- Alexander L. Turner

Data Breach Costs Spread Downstream, IBM Says

"Nearly half of all organizations studied by IBM have minimal or no cloud security practices in place."

Why this is important: In 2022, the global average cost of a data breach increased to $4.35 million. IBM's recent Cost of a Data Breach report revealed that the average cost of a data breach of an American company is $9.4 million. Those numbers likely cause the reader sticker shock. However, the report offered more. It also proposed that the full cost of any data breach is more than the publicized average

cost. One of the main reasons for this, it reports, is the fact that many organizations that suffer a data breach pass the cost onto their customers. --- Nicholas P. Mooney II

Ex-CFTC Chairman Discusses Celsius' Bankruptcy and CBDC Adoption

"The former Commodity Futures Trading Commission chief joined CoinDesk TV's 'First Mover' to discuss why the bankruptcy of lender Celsius Network could set legal precedent in future crypto hearings, and why the likelihood of CBDC adoption worldwide could be based on Chinese technology."

Why this is important: Celsius Network is a New Jersey-based cryptocurrency lending platform that has recently filed for Chapter 11 bankruptcy protection in the Southern District of New York. Seeking to restructure and hopefully emerge from bankruptcy, the company's bankruptcy case represents a significant development as crypto gains a foothold in United States markets. The bankruptcy proceedings will be important to monitor as they may set a course for future bankruptcy cases where crypto-based assets are a large factor. This could become even more significant as support grows for the development of a central bank digital currency ("CBDC") in the United States. China has already instituted a digital yuan that is available to early adopters. There are currently about 250 million digital wallets holding digital yuan. Implementing a CBDC in the United States would certainly raise privacy concerns. The technology underlying the digital yuan is powerful in that it can be adapted to a wide variety of devices and digital assets, but it also lends itself to increased surveillance and censorship issues. While there is no current decision of the Federal Reserve to create a CBDC in the United States, the idea is being explored and discussed. In a recent paper titled Money and Payments: the U.S. Dollar in the Age of Digital Transformation, the Federal Reserve addresses the need for an open dialogue and comment among consumers, lawmakers, and regulators on the potential benefits and risks of implementing a CBDC in the United States. The initial 120-day comment period on the paper has closed, but questions are still able to be submitted by interested parties. --- Brian H. Richardson

FBI Issues New Alert about Stolen Academic Credentials Found Online

"The agency says colleges and universities should take steps to detect anomalies on their networks and prevent future attacks."

Why this is important: Advances in technology increase the potential risk exposure for private and public educational institutions. In a recent alert, the Federal Bureau of Investigations has detailed a practice called "credential harvesting," where cybercriminals obtain login information through a number of targeted cyberattacks. These credentials are used for "brute-force credential stuffing," which allows cybercriminals to input the stolen information into other website login forms to gain access to user accounts. The FBI urges educational institutions to implement and maintain cybersecurity training, multifactor authentication, and other necessary measures to protect personal data of anyone affiliated with the institution. As these cyberattacks become increasingly more common, institutions should consider installation of a third-party security software to monitor, detect, and block potential threats to their networks. --- Kelsie A. Wiltse