SHARE:

Join Our Email List

View as Webpage

March 17, 2022

Welcome

Welcome to the fifth issue of *Decoded* for the year.

We are very pleased to announce that our Technology Practice Group is growing as we have recently welcomed two new attorneys to the firm.

Alison M. Sacriponte is a Counsel attorney in our Pittsburgh office. Her primary areas of practice are corporate, business, and technology law. Alison received her B.A. from Duquesne University; her J.D. from the University of Pittsburgh School of Law; and her LL.M. in International Legal Sciences from Universitat Pompeu Fabra, Barcelona. She is admitted to the Pennsylvania Bar. Alison is fluent in Spanish, and she has spent most of her career serving clients in the internet and technology industries.

Alyssa M. Zottola is an Associate attorney in our Pittsburgh office. Her primary area of practice is litigation with a specialized interest in technology issues. She received her B.A., *magna cum laude*, from the University of Pittsburgh and her J.D. from the University of Pittsburgh School of Law. She is admitted to the Pennsylvania Bar. Alyssa is fluent in Italian.

At Spilman, we are dedicated to providing the services needed to address all of your legal issues. The addition of these two attorneys helps us attain an elevated level of service. Please join us in welcoming them both to the firm!

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

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

and

Alexander L. Turner, Co-Editor of *Decoded*

The Cryptocurrency Revolution and President Biden's Formal Recognition

By Ronald W. Schuler

Out of the ashes of the 2008 financial crisis, Bitcoin sprang up like an insurgency, targeting both the unbridled activity of large financial institutions and the monetary policies of governments charged with overseeing them. The goal of the developers and early adopters of cryptocurrency was to unseat a reserve currency (the dollar). After more than a decade of derisive mirth and skepticism over the idea of cryptocurrency, an organically evolving trading market that was capable of producing a swagger of crypto billionaires (overnight, intermittently), and a chaotic U.S. regulatory approach, one certainty has emerged: the financial institutions that were once the targets of the developers and early adopters have moved from being crypto denouncers to becoming crypto advisors and crypto investors.

Click **here** to read the entire article.

Three Cybersecurity Companies to Offer Free Protection to U.S. Hospitals and Utilities Amid Concerns of Hacking Attacks

"Though no surge in cyberattacks on American companies has been reported, the federal government's Cybersecurity and Infrastructure Security Agency has urged U.S. organizations to lock down their systems in case the Russian government or private hackers take action as the divide between Russia and the United States grows."

Why this is important: Your business may be at risk of becoming a casualty of the war in Ukraine by way of a Russian cyberattack. That is the warning that the federal Cybersecurity and Infrastructure Security Agency issued to U.S. businesses recently. While it does not appear that Russian cyberattacks have increased at this time, the federal government cautions that as economic sanctions take hold, Russia may lash out in retaliation. This may include cyberattacks on vulnerable industries by Russian state actors or private entities on Russia's behalf. In response to the federal government's warning, three cybersecurity companies, CrowdStrike, Ping Identity, and Cloudflare, are attempting to capitalize on the risk posed by possible Russian retaliation by offering four months of free cybersecurity services to new customers in industries that are most at risk of cyberattacks, which include utilities, financial systems, and the healthcare industry. While these offers are enticing, the article also points out that two of the three companies also do work, to varying degrees, in Russia. Being mindful of possible conflicts of interest your cybersecurity vendors may have is something you need to consider as part of your cybersecurity plan. Whether you decide to take these companies up on their offers or not, a proactive approach to cybersecurity is always the best course of action, and your organization should have a robust cybersecurity plan in place to ward off bad actors regardless of current geopolitical events. --- Alexander L. Turner

---

UC Berkeley Loses CRISPR Patent Case

"The decision stymies years of efforts from the University of California, Berkeley to obtain lucrative patent rights to the technology."

Why this is important: This article is a short and clear description of the current status of a long fight between UC Berkeley and MIT/Harvard's Broad Institute relating to a patent for CRISPR-Cas9 used on human genes. There is little question that Jennifer Doudna of UC Berkeley (with Emmanuelle Charpentier, now of Max Planck Institute) invented CRISPR-Cas9 for gene editing, and later won the Nobel Prize for that in 2020. Broad Institute, however, filed the first patent on use of CRISPR on human gene editing. UC Berkeley objected, and the dispute was on! I am not qualified to speak to the merits of this, but many fledgling companies have bet on one side or the other, obtaining a license from either UC Berkeley or Broad Institute.

The final result of this (now favoring Broad Institute) may create damage to all of the companies who rely on licenses from the "wrong" side. Why? Well, if the licensor cannot deliver the IP, that license probably terminates. Then the licensee must negotiate a new license with the other party (who can deliver the IP). That will be expensive! First, the licensee has been using the IP for years (probably) without authority. There's a cost to that. Second, a license to a startup company with a narrow

application of the IP generally will be much cheaper than a necessary license negotiated when the product is already into clinical trials. This is especially true if that IP is unique to development and manufacture of the product. This could kill promising drugs, depending on how "retributive" Broad Institute is in pursuing its patent. Even if Broad Institute is reasonable (generous?) under the circumstances, the license price for a later-stage product should be more, and it may require changes in other licensors for that product. This creates possible royalty stacking issues not already priced into the drug. This truly is an awful mess. --- Hugh B. Wellons

---

Crypto Awaits Judgment on LBRY Coin

"LBRY, a blockchain-based file sharing and payment network, has been the subject of a yearslong case by the SEC."

Why this is important: LBRY is a blockchain-based file sharing and payment network that allows uncensored and unlimited digital content sharing and allows consumers to tip content creators through LBC, its token currency. The SEC has sued LBRY, claiming LBC is a security and should have been registered as such. LBRY claims a win for the SEC could impact all cryptocurrencies, and it intends to continue to defend the claims. The SEC's pursuit of LBRY, which has been likened to Javert's relentless pursuit of Jean Valjean, doesn't appear headed toward settlement. This lawsuit highlights some of the uncertainty in cryptocurrencies that the recent executive order from the Biden Administration hopes to address. --- Nicholas P. Mooney II

Data Privacy Laws are an Opportunity to Become More Honest in Reaching Your Target Audience

"Data privacy regulations are designed to give consumers more transparency into and control over how their data is collected, shared and used, especially as more consumers grow concerned about how their data is accessed and used by big data companies."

Why this is important: American consumers are becoming increasingly aware (and increasingly concerned) with how their data is being collected and used by companies both large and small. Interestingly, the United States does not have a specific policy to address and enforce data privacy protection. Unlike the European Union's General Data Protection Regulation (a comprehensive privacy policy that went into effect in May 2018, giving Europeans greater control over how businesses access and use their data), the United States has an amalgamation of policies intended to protect certain types of data, such as health care (with the Health Insurance Portability and Accountability Act). California has attempted to emulate the European Union by passing the California Consumer Privacy Act, a comprehensive privacy policy that gives consumers greater control over how their data is collected and used by companies conducting business in California. Colorado and Virginia also have enacted similar policies.

Companies that conduct business in California, Colorado and Virginia need to be aware of the heightened standard those states expect of businesses that handle consumer data and if that meets the applicable standard. While there is not an overarching Federal Data Privacy law, and the three states have different standards that companies need to meet, businesses can use this opportunity to implement a more stringent data privacy standard. Complying with the most stringent standard would ensure that companies also comply with the states with less stringent data privacy protection requirements. Additionally, by proactively implementing stringent data protection policies, companies will work to build consumer trust. As consumers are more concerned about how their data is being handled, hearing from a company directly that it is taking active steps to protect their data is bound to create consumer goodwill. --- Alyssa M. Zottola

---

First Surgeries Completed with In-Hospital Metal 3D Printed Implants

"The aim of this innovative, first of its kind project is to provide faster and more accessible care for U.S. patients requiring personalized and unique complex joint replacement solutions."

Why this is important: This was bound to happen. It's a description of just one example of a company combining surgery and engineering to measure and make a special implant by 3D printing, designed to fit a particular patient in joint reconstruction. This may shorten the process time for joint reconstruction and will be particularly helpful in trauma cases. --- Hugh B. Wellons

---

Medical Device Disclosures on the Rise, but Providers Struggle to Patch Known Flaws

"Healthcare organizations also struggle to maintain strong patch management policies able to swiftly remediate vulnerabilities after disclosure, despite a number of federal and private sector efforts to support and educate providers with remediation."

Why this is important: The Internet of Things can result in the collection of very personal information. In the case of networked pacemakers, infusion pumps, and other medical devices, this collection of data becomes even more personal because these devices become part of you and transmit your vital health information. While the networkability of these devices enables doctors to have real-time access to important health information, this same convenience also has its risks. It is becoming increasingly apparent that these networked medical devices are susceptible to computer viruses, malware, ransomware, and hacking by bad actors. Due to the increase in vulnerability disclosures, it has become clear that many networked medical devices have software vulnerabilities that can put a patient's life in danger. However, manufacturers and IT specialists are unable to keep up with the necessary software patches to remedy these known vulnerabilities. The result is that medical devices with known flaws are being implanted in patients with the hope that the faulty software will be able to be updated at some point in the future before an adverse cyber event can occur. While the loss of PII as a result of a cyberattack on a medical device is not desirable, the risk that a bad actor could implant ransomware to hold thousands of patients' implanted medical device hostage is absolutely terrifying. Thankfully, the vulnerabilities in these devices have not yet been exploited by bad actors. However, the risk remains, and the question of liability in the event of a compromised medical device is still unclear due to lack of litigation on the issue. The device manufacturer would have possible liability for design defect, manufacture defect, and failure to warn regarding the known, but unresolved, security issues with the implanted device. These vulnerable medical devices also may create a new form of liability exposure for medical providers. The best course of action at this time is to get the vulnerabilities in these devices patched as soon as possible to avoid the devices being compromised in the future. --- Alexander L. Turner

---

3 Key Elements of a Data Protection Impact Assessment

"A data protection impact assessment (DPIA) is becoming an increasingly important tool for identifying, investigating and mitigating risks related to consumer privacy."

Why this is important: As the value of consumer data continues to skyrocket, consumers are increasingly wary of their data being collected, with growing concerns about data privacy and cybersecurity. If companies want to continue reaping the widespread benefits of access to consumer data, they must enhance their privacy policies and practices, establish transparency, and build trust with their consumers. A data protection impact assessment ("DPIA") is an indispensable tool for identifying, investigating and mitigating risks, enabling companies to better understand the nature, scope, context and purpose of their data processing. While many government privacy regulations (such as the GDPR and CPRA) already mandate that businesses carry out DPIAs, companies should anticipate this requirement expanding. Rather than consider it a compliance checkbox though, companies can use the DPIA to gain a thorough understanding of their data flow, the intersection of consumer rights, and how to manage a privacy regime. Such posture is rooted in digital ethics, but it also stands to improve customer relationships and, ultimately, revenues. --- Alison M. Sacriponte

---

FDA Final Guidance Presses Industry to be 'Recall Ready'

"FDA has finalized guidance on the preparations companies should take to ensure they quickly and effectively execute voluntary product recalls."

Why this is important: Most of life is a series of "good news, bad news." The FDA is making huge strides improving the efficiency of its drug and medical device approval process. That, in addition to recent manufacturing problems and other issues, however, is resulting in more frequent recalls. This article describes the final FDA guidance requiring companies to have a practical plan in hand to initiate recalls quickly and effectively. In a second article in the same publication, the FDA also is requiring U.S.-approved manufacturers to switch from the current FDA quality guidance to the international standard, which aligns with "Devices Good Manufacturing Processes" in the future. Many manufacturers already satisfy both standards, but some do not. This may be an expensive and time-consuming process for them. --- Hugh B. Wellons

---

Poor Employee Cyber Hygiene is Putting Healthcare Cybersecurity at Risk

"Risky employee behaviors need to be eradicated and the workforce needs to be trained to be more security-aware and taught how to recognize common attacks that target individuals, such as phishing and social engineering."

Why this is important: Cybersecurity is only as strong as its weakest link, and the weakest link in many healthcare organizations is often the organizations' own employees. With the rise of hacking events, ransomware attacks, and vulnerability disclosures in 2021, healthcare organizations must focus on improving their employees' privacy and data security training and behaviors. Poor security awareness training has been a significant contributor in the rise of privacy and data breaches in the healthcare industry. The result is that employees often circumvent inconvenient security protocols, which result in the organization becoming vulnerable to attack. These workarounds include using personal devices, and unregulated apps and services, like Gmail and Dropbox, while working with PII and PHI. Password hygiene also remains a major security risk, with 80 percent of cyberattacks resulting from compromised network passwords. These are issues that need to be addressed with more robust training to remove these risky behaviors from the work flow and to show employees why these activities endanger network security. Additionally, healthcare organizations should be "conducting risk analyses, having robust risk management practices, conducting vulnerability scans, and implementing technical safeguards such as intrusion prevention systems, next-generation firewalls, and spam filters" in order to protect their networks. Providing this training and increased network security will lessen the chance of a HIPAA violation and the cost of addressing a data breach. --- Alexander L. Turner

---

Weight Management Companies Settle Data Privacy Suit

"Two American weight management companies have agreed to pay $1.5m to resolve allegations concerning the illegal harvesting of children's sensitive data."

Why this is important: The Children's Online Privacy Protection Act ("COPPA") and the Children's Online Privacy Protection Rule ("COPPA Rule") impose certain requirements on operators of websites or online services that are child-directed or knowingly collect personal information from children. Businesses that provide services that fall within COPPA must provide notice of their information practices; obtain verifiable parental consent prior to the collection, use or disclosure after providing a means for the parent to view the information; and maintain reasonable procedures to protect the confidentiality, security and integrity of the personal information, as well as other requirements.

In a settlement with the Federal Trade Commission, Kurbo, Inc. and Weight Watchers International have agreed to delete personal information illegally collected or maintained, destroy the algorithms derived from the data and pay a penalty. This suit should serve as a reminder to businesses that they must assess whether or not they fall within COPPA and if so, determine what practices they need to incorporate to ensure compliance. --- Annmarie Kaiser Robey

---

Critical Bugs Expose Hundreds of Thousands of Medical Devices and ATMs

"The so-called Access:7 vulnerabilities are the latest high-profile IoT security fumble."

Why this is important: A recent acquisition uncovered seven vulnerabilities in medical devices that could place a patient, or an entire network, in danger. Alex Turner has addressed this, as well, in *Decoded*. If you are in this business, cybersecurity must become a mantra. --- Hugh B. Wellons

---

Fintech Scams Promise Windfall for Crime Prevention Firms

"Silent Eight, a Singapore-based financial crime prevention firm, announced that it had raised $40M in Series B funding."

Why this is important: In 2020, regulators imposed more than $6.8 billion in fines against 28 financial institutions in 14 countries as a result of what they saw as inadequate anti-money laundering procedures. The desire to avoid fines like these and to project a commitment to robust anti-money laundering programs is helping financial crime prevention firms like Silent Eight raise funding. The funding is attracting well-known names like HSBC. Its venture funding affiliate HSBC Ventures, already a client of Silent Eight, invested in its latest round of funding. With bad actors looking for more creative ways to hide money laundering, terrorist financing, and human trafficking, and with the potential for large penalties to financial institutions that fail to notice their activities, expect firms like Silent Eight to continue to have a market for their services. --- Nicholas P. Mooney II

To Test Cancer Drugs, These Scientists Grew 'Avatars' of Tumors

"Growing organoids in dishes and xenografts in mice lets scientists re-create a living person's tumor—and test dozens of drugs against them at the same time."

Why this is important: This science is way beyond my ken, but I believe that this explains how scientists are growing cancers in a lab, inserting them into DNA-altered mice, and then testing various treatments to see which work best. This may create both a way to develop better cancer treatments and also how to find more effective treatments for very rare/unique and difficult cancers. --- Hugh B. Wellons

---

Chinese Spies Hacked a Livestock App to Breach US State Networks

"Vulnerabilities in animal tracking software USAHERDS and Log4j gave the notorious APT41 group a foothold in multiple government systems."

Why this is important: Surprise, hackers are very creative! This article describes how Chinese hackers used animal tracking software to get a foothold in state government systems. Animal tracking software helps state governments track and predict animal disease outbreaks and other such issues. These systems also connect to other, more sensitive, government systems. A notorious Chinese cyber-spy hacked into the tracking software for animals and used that to springboard into other state government systems, at least six of them. Scary article. --- Hugh B. Wellons

---