SHARE:

Join Our Email List

View as Webpage

April 28, 2022

Welcome

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

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

Brian H. Richardson is an Associate in our Roanoke office. His primary areas of practice are commercial disputes, workouts, and related litigation, with an emphasis in corporate restructuring, bankruptcy, creditors' rights, and health care finance matters. He received his B.S. from Brigham Young University and his J.D. (with a Certificate in Law, Science, & Technology) from Arizona State University Sandra Day O'Connor College of Law, where he also served on the Executive Board for *Jurimetrics: The Journal of Law, Science & Technology*. He is admitted to the Virginia Bar, the United States District Courts for the Eastern and Western Districts of Virginia, the United States Bankruptcy Courts for the Eastern and Western Districts of Virginia, and the United States Court of Appeals for the Fourth Circuit. Brian is also fluent in Spanish.

Jacquelyn N. Miner is an Associate in our Winston-Salem office. Her primary area of practice is litigation. Jacquelyn received her B.A. from Mars Hill University and her J.D. from The College of William and Mary Marshall Wythe School of Law. She is admitted to the North Carolina State Bar.

Kelsie A. Wiltse is an Associate in our Winston-Salem office. Her primary areas of practice are litigation and employment law. She received her B.A. from University of North Carolina at Charlotte and her J.D. from Elon University School of Law. Kelsie is admitted to the North Carolina State Bar.

We are dedicated to providing the services needed to address all of your legal issues. The addition of Brian, Jacquelyn and Kelsie helps us attain an elevated level of service. Please join us in welcoming them 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*

Data Breach Corner

Cash App Data Breach Affects More than 8M Users

"A former employee of the company downloaded reports containing the personal information of U.S. users."

Why this is important: Not all data incident threats come from outside a company. In this case, Cash App recently reported that more than 8.2 million users had personal information exposed at the end of last year. The information includes the customers' full names, account numbers, and in some instances their portfolio value, holdings, and trading activity. This information was compromised not by a sophisticated threat actor hacking the system to look for a payday, but rather by a former employee. Cash App's parent company Block discovered that a former employee downloaded the information after the employee's contract ended. The employee had access to the data as part of their job duties, but the article doesn't explain how the employee still was able to access the data after their contract ended. Cash App currently is investigating this incident. This article underscores the need for companies to have protocols in place regarding data security when employees leave a company.

Decoded usually reports on articles related to data breaches, and this issue does the same. However, we found several additional articles related to data breaches we flagged as significant, but were not able to report on in this issue. We're including links to them here for further reading. The number of articles tells us the significance of this issue and how seriously companies and individuals should treat it. --- Nicholas P. Mooney II

SuperCare Health Sued Over 318,000-Record Data Breach
UKG Hack Fallout Includes Lawsuits, Data Breaches
Patients Increasingly Suing Hospitals Over Data Breaches
Big Coral Gables Mortgage Servicer Hit by Data Breach, Exposing Clients' Personal Information
Data Breach Goes Unnoticed For Nearly 1 Year at KS Hospital

Drafting Patent Acquisition Agreements

By William P. Smith

Companies may purchase third-party technology from time to time. When acquiring patents from outside the company, or from related entities, there are important factors to be considered. Here are certain issues for buyers when preparing a patent acquisition agreement.

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

Cybersecurity Litigation Risks: 4 Top Concerns for CISOs

"What litigation risks should CISOs be most concerned about and what can they do about it?"

Why this is important: Corporate Information System Control Officers ("CISO") are tasked with administrating their corporations' IT infrastructures. This includes protecting against attacks and the disruptions such attacks have on the normal functions of the business, including the legal implications of a data breach. Data breaches have been on the rise, and CISOs have anticipated that the increase in data breaches will be a significant driver in corporate legal disputes moving forward. The article addresses four concerns for CISOs related to data breaches: (1) increased civil litigation; (2) customers and shareholders holding the CISO personally liable for the breach; (3) the loss of trade secrets; (4) the lack of a universal federal cybersecurity law that addresses data security and data breaches.

While this article discusses that data breaches are on the rise along with corresponding lawsuits, the article does not discuss recent court decisions having tempered the risk of litigation. In recent issues of Decoded, we have discussed court decisions that have limited plaintiffs' abilities to bring an action following a data breach. Courts have held that the fear of a future harm in the form of identity theft does

not constitute an injury-in-fact that conveys standing to bring a suit. Claims related to a data breach require the plaintiff to show a concrete injury-in-fact and not just a speculative injury that may manifest at some point in the future. Courts have also recently held that companies are not required to absolutely protect customers and employees' PII, but that they only need to take "reasonable" steps to protect the data they maintain. The take-away from these recent rulings is that not every data breach, while disruptive and a potential black eye for the corporation, will result in a large settlement or verdict. Any litigation, even if you ultimately are successful, will be costly. Know that if a breach does occur that litigation will likely follow even if you did everything right.

CISOs have reason to worry about being held liable by customers and/or shareholders following a data breach. While this article addresses the liability a CISO may have following a data breach, it does not address the actions a CISO can take to mitigate those risks. A CISO has to be proactive and implement reasonable cybersecurity protocols to protect the corporation's IT infrastructure. A CISO must also communicate potential risks and breaches in a timely fashion to upper management and the Board of Directors so that they can take appropriate actions to address those risks. The CISO must also be aware of the contents of the corporation's privacy policy and notice to ensure that what the corporation is promising in those as steps its taking to protect PII are being followed. Additionally, the CISO should be up-to-date with industry specific laws and regulations that address data breaches and required notice provisions to ensure that those procedures and notice deadlines are included in the data breach response plan, and that the data breach response plan is strictly adhered to in the event of a data breach. CISOs are also recommended to retain counsel experienced with handling data breaches and cybersecurity litigation to help guide the CISO through the process. Taking these actions will lower the risk of a CISO being found personally liable following a data breach.

The loss of trade secrets and reputational damages as the result of a data breach are significant consequences of a data breach. Pre-planning is the best way to avoid the risk of the loss of trade secrets and damage to the corporation's reputation as a result of a data breach. This includes implementing protocols and procedures that would protect the corporation's IT infrastructure from attack. This plan would include mandatory employee training on preventing the disclosure of sensitive information, conducting third-party cyber assessments for all vendors, segregating sensitive information and requiring additional authentication to limit access to that information, and having a plan in place to routinely monitor new risks to the system. Having a robust plan in place to prevent a breach is the best protection from the loss of trade secrets or the loss of reputation as the result of a data breach.

The lack of a comprehensive federal cybersecurity law is concerning. Many industries have industry-specific data security statutes and regulations, like the healthcare industry and HIPAA, and the financial industry and FCRA. Unlike in the EU with the GDPR, there is not one law or regulation to which a CISO can turn to get guidance on what data security steps the corporation must take to protect PII, or what a CISO must do in the event of a data breach. CISOs must know what laws and regulations govern their specific industries, and what those laws and regulations prescribe regarding data security and data breaches.

Cybersecurity is a complex and confusing issue that requires continued diligence and learning. By being proactive, CISOs can limit the risks of a data breach and subsequent litigation. --- Alexander L. Turner

---

LVMH Collects People's Facial Scans without Asking When They Use Its Virtual Try-On Tool for Glasses, Lawsuit Claims

"The Louis Vuitton North America unit is accused in the suit of collecting 'detailed and sensitive biometric identifiers and information, including complete facial scans.'"

Why this is important: The lawsuit discussed in this article is one of the latest to be filed under Illinois's Biometric Information Privacy Act ("BIPA"). The act requires companies and parties to obtain the informed consent of an individual prior to obtaining their biometric information, as well as inform them of how the information will be stored and the purpose for which it will be used. It provides a party with a private right of action for an individual to bring suit and $5,000 fines (plus attorney's fees) for a reckless violation of the statute. In this case, the plaintiffs allege that LVMH (the parent company of Louis Vuitton) collected biometric information of customers who used their "virtual try-on tool" to try on sunglasses without first obtaining their consent to collect the information.

It is not uncommon for retailers to offer customers an option to virtually "try on" a product before buying it, or virtually place a product in a space prior to purchasing the product. Retailers conducting business in Illinois, Texas or Washington should be particularly cautious of how they are collecting and maintaining biometric data from customers in those states. Decoded has repeatedly discussed new lawsuits arising

under Illinois's Biometric Information Privacy Act, which differs from Washington and Texas in that it provides a private right of action and allows for $5,000 penalty per violation. That is not to say that retailers should not offer customers the opportunity to virtually try on products. Rather, it is a reminder that retailers should seek the informed consent (explicitly stating how the data will be collected and held) of the customer prior to collecting the data in order to protect themselves from violating Illinois's privacy act and other biometric information privacy policies. --- Alyssa M. Zottola

---

Open Sharing of Biotechnology Research—Transparency Versus Security

"The authors grapple with a critically important issue that emerged with the advent of nuclear physics: how the scientific community should react when two values—security and transparency—are in conflict."

Why this is important: Open science makes it possible for scientists and researchers to cure illnesses, prevent diseases, and even quickly produce effective vaccines in response to a pandemic. But, at what cost? While open science is invaluable to producing and disseminating reliable and efficient research, there is a range of biosafety and biosecurity implications. There is a somewhat obvious need to protect certain research projects and results from wide distribution, like the engineering of nuclear weapons, as the distribution of this research would make it easier for a bad actor or terrorist to reproduce the weapon and use it for nefarious purposes. For the biotech industry, the security concerns may not be as obvious, but any misuse could have an equally destructive, if not greater impact, including the accidental release of an existing virus, and/or the creation of new viruses or chemical weapons. However, the need to protect this information must be balanced with the need to share this information as science is most efficient and reliable when it is accessible, verified, and reused. The scientific community will need to take steps to mitigate the potential risks from any intentional or accidental misuse. --- Jacquelyn N. Miner

---

Envision Glasses for the Blind Can Read Documents, Scan Faces, Aid Navigation

"Smart glasses from Envision are built on the enterprise edition of Google Glass."

Why this is important: Envision Glasses provide individuals who are blind or have low vision with the opportunity to experience their surroundings by speaking the information to the user. The glasses can read and speak short or long sections of text, describe one's surroundings or assist with a video call. The glasses are a headset hands-free design that works with Google Glass Enterprise Edition 2. The glasses have a camera, run on a battery and connect with Wifi and Bluetooth. This innovative approach allows the user to exercise greater independence with a user-friendly design. As technology continues to improve, it is anticipated that additional features will be added to improve the users' everyday lives and facilitate greater communication with those they encounter. --- Annmarie Kaiser Robey

---

FDA Official: Draft Cybersecurity Guidance has 'Teeth' and The US is Trying to Fix Medical Devices' Big Cybersecurity Problem

"Not following the guidance in premarket submissions means potential delays for device makers, said Suzanne Schwartz, director of CDRH's Office of Strategic Partnerships and Technology Innovation."

"The FDA and Congress both just put out new proposals."

Why this is important: In a previous issue of Decoded, we discussed the alarming fact that many medical devices, including those that are implanted in patients' bodies, are leaving the manufacturer with known cybersecurity flaws. Due to these known flaws, these devices are vulnerable to being hacked, and patients' PHI stolen, or worse, the device being held hostage in a ransomware attack. Luckily, these worse case scenarios have not come to fruition. Now that they are aware of these risks, Congress and the FDA are stepping in to provide guidance to device manufacturers on closing these cybersecurity gaps. For years, the FDA has been working with device manufacturers requesting feedback on how to best protect against cyber threats, and providing the industry with voluntary guidelines on how to implement

greater cybersecurity. The FDA issued a final cybersecurity guidance in 2014 addressing premarket expectations in 2014 and complementary post-market guidance in 2016. Because of rapidly advancing cybersecurity threats, the FDA recently issued guidance that addresses a total product lifecycle approach to cybersecurity and the implementation of a Software Bill of Materials ("SBOM"). A SBOM allows the device manufacturer, clinician, medical facility, and patient to better monitor whether the device they are using, wearing, or that was implanted may contain compromised software. This will allow the user of the device to know that any specific medical device has a vulnerability and request a software patch from the developer of that software. The FDA has also gone to Congress to ask for greater authority to regulate this issue and allow the FDA to issue mandatory regulations. Earlier this month, Congress introduced the Protecting and Transforming Cyber Health Care Act ("PATCH Act"). The PATCH Act would allow the FDA to issue mandatory guidelines governing cybersecurity for medical devices. This would establish the FDA's "authority in the area of cybersecurity and tie that directly to the safety of medical devices." However, the PATCH Act will only apply to new devices and not to older devices that are already being used in the market. While the PATCH Act is a good step in the right direction, there are millions of patients whose health remains at risk because of medical devices that remain vulnerable to a cyberattack. --- Alexander L. Turner

---

FDA Authorizes First COVID-19 Breathalyzer Test, Clearing Path to 3-Minute Results

"FDA expects the test to be run at doctors' offices, hospitals and mobile testing sites."

Why this is important: As the United States enters the "control phase" of its response to the COVID-19 global pandemic, the hope is that protective measures become less invasive as time goes on. A new emergency use authorization issued this month by the FDA seeks to do just that. InspectIR Systems, LLC, is a Texas-based research company focused on developing portable diagnostic screening and testing equipment. Using an analysis of five volatile organic compounds identified as being associated with SARS-COV-2 viral infection, the company has developed a portable device for testing for the virus in a patient's breath, with results in three minutes. The test analyzes breath samples of 0.25L using gas chromatography and a quadrupole mass spectrometer. This is not your typical hand-held breathalyzer, though. The device is about the size of a standard carry-on, and the FDA expects the test to be administered by trained staff at healthcare facilities. Results are not to be deemed conclusive for any individual. A positive result is a "presumptive positive" and should be followed by a molecular test. A negative result should be considered in the full context of "recent exposures, history, and . . . clinical signs and symptoms consistent with COVID-19." Time will tell how the FDA's expansions of emergency use authorizations arising from the pandemic may shift the approval landscape going forward for other indications as well. --- Brian H. Richardson

---

Coinbase Launches NFT Marketplace in Beta

"Testers can crack open their crypto wallets to browse, buy or sell art."

Why this is important: Non-fungible tokens have experienced a bumpy ride recently. The average sale price of an NFT is now below $2,000, down from an average sale price of almost $7,000 in January. However, the number of NFT transactions continues to rise, and the number of possible use cases for NFTs continues to expand. This article reports on Coinbase's beta testing of its NFT marketplace in which creators of digital art and buyers will be able to interact on a peer-to-peer basis. Coinbase reports that it plans to add token-gated communities and other features to its NFT offerings in the coming months. Coinbase is the largest cryptocurrency exchange in the U.S. Its plan to add an NFT marketplace, especially where its NFTs have practical use cases, could be a boost in helping the NFT market weather its bumps and continue to grow. --- Nicholas P. Mooney II

Employee Email Warnings Reduce EHR Snooping, Unauthorized PHI Access

"Employees who received an email warning after unauthorized PHI access were far less likely to commit the same offense again, research published in JAMA found."

Why this is important: Curiosity killed the cat, and in a healthcare setting, employee curiosity regarding patients leads to a HIPAA violation. Only those employees who are on the patient's care team have authority to access that patient's medical records. How do you stop employee lookie loos who have access to patient records from perusing patients' PHI? Let them know that they are being watched. How do you do that? By having your records management system notify the offending employee via a follow-up email that they have engaged in an unauthorized access of a patient's medical records. A study in 2018 found that only 2 percent of healthcare employees re-offended after receiving an email warning them that their access of a specific patient's medical records was unauthorized. Since employees are one of the largest threats to a business' cybersecurity, implementing this type of warning system may be equally effective outside of the healthcare setting. If an employee is aware that they are being monitored, and are informed that their illicit activity has been identified, he or she is less likely to try and access restricted information. --- Alexander L. Turner

---

Tech Giants Duped into Giving Up Data Used to Sexually Extort Minors

"The companies that have complied with the bogus requests include Meta Platforms Inc., Apple Inc., Alphabet Inc.'s Google, Snap Inc., Twitter Inc. and Discord Inc., according to three of the people."

Why this is important: Criminals have become increasingly more innovative in finding ways to obtain individuals' personal identifiable information ("PII"). The latest scam is for criminals to fraudulently represent themselves as law enforcement officers and submit emergency data requests to social media companies in order to obtain targeted subscriber's PII. Often, these criminals are targeting women and minors. Responses to these requests generally include a subscriber's name, IP address, email address, and physical address. The criminals then use this information to befriend the victims and after gaining their trust, they encourage the targets to send the criminals sexually explicit photographs and videos that are later used to blackmail the victims. When targets of this scheme balk at providing the requested photos and videos, they have been subjected to severe harassment in retaliation for failing to comply with the criminal's request.

It is almost impossible for even large and sophisticated tech companies to parse out fraudulent emergency data requests from the legitimate requests made by law enforcement officials. This is in part due to criminals exploiting the legal process and issuing sham subpoenas, and forging judges' signatures. These criminals are taking advantage of the large number of emergency requests these social networks receive every day. It is important for your company to verify the validity of any law enforcement request or civil subpoena that requests individuals' private information. If your company receives an emergency data request or civil subpoena, it is important that you are aware of this new scam, and that you properly vet all law enforcement requests and warrants, and civil subpoenas requesting individuals' PII before providing that information to the requesting party. Even if the request is valid, industry specific laws and regulations may prevent you from providing the requested information. If you have any questions regarding the validity of such a request, or if you are legally permitted to provide the requested information, Spilman's Technology Law Practice Group is available to assist you. --- Kelsie A. Wiltse

---

Scientists Finally Finish Decoding Entire Human Genome, New Blood Stem Cell Road Map Helps Scientists Learn from Mistakes on Quest to Create Cells in Lab and Garuda Thinks It has Cracked the Code to Off-the-Shelf Stem Cell Transplants—and Investors are Betting $72M to Find Out

"The previous effort, celebrated across the world, was incomplete because DNA sequencing technologies of the day weren't able to read certain parts of it."

"Researchers at the University of California, Los Angeles (UCLA) have unveiled a novel road map tracking blood stem cell development in the human embryo, findings that could help develop new treatments for blood cancers and inherited blood disorders."

"Equipped with the platform, Garuda wants to eliminate the need for healthcare providers to find matched donor materials or use a patient's own cells."

Why this is important: Human DNA was decoded originally by December 1999. We had some understanding of what most genes did, but there were holes in the analysis. Researchers have been working ever since to fill in the holes. Accordingly, when we first began to replace or change genes, it often was "rough science," not precise science. There were unintended consequences that could be severe. This more complete picture is critical to better genetic science. In conjunction with this effort, researchers at UCLA and at Garuda, a Boston biotech company, have been using a more complete "roadmap," and developing that to some degree focuses on their target, to create better processes for growing blood and other stem cells. Stem cells can help to heal and grow back certain tissues in the body, but they often have to be "coded" for the individual to be effective. That is an expensive treatment. As researchers develop better means to "grow" these stem cells from the individual's blood or other tissues, the cost should go down while efficacy improves. --- Hugh B. Wellons

---