SHARE:

Join Our Email List

View as Webpage

May 12, 2022

Welcome

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

We are very pleased to announce that 13 of the firm's West Virginia-based lawyers were recognized by Super Lawyers on the 2022 West Virginia list. The objective of the Super Lawyers selection process is to create a credible, comprehensive and diverse listing of outstanding attorneys from more than 70 practice areas. Several of these attorneys practice within the technology realm, and you can see a comprehensive listing here. Congratulations to those honored, and we hope this recognition instills a sense of confidence in our skills and insights.

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*

Avoiding Data Breaches: A Guide for Boards and C-Suites

"Recently, plaintiffs have targeted corporate board members and C-level executives alleging that their data privacy–related claims result from a breach of fiduciary duties."

Why this is important: Corporate board members and C-level executives cannot hide their heads in the sand when it comes to data security. A data breach can have a significant monetary and reputational impacts on the company. Consequently, they risk being named in suits brought by customers whose personal data was exposed as a result of the breach and by shareholders alleging that the board members and executives breached their fiduciary duty to protect the plaintiffs' personal information or that they unnecessarily exposed the company to liability. There are steps that board members and C-level executives can take to protect their company from data breaches and themselves from liability. The first

step is to implement technology solutions, including quantum computing and quantum-resistant encryption, zero trust security, and zero knowledge proofs. Quantum computing and quantum encryption can generate truly random numbers for encryption keys, which prevents hackers from cracking the company's encryption. Some privacy laws incentivize encryption, like the California Consumer Privacy Act, by stating that a company's failure to encrypt personal information can result in a direct cause of action by customers in the event of a data breach. Zero trust security is used to mitigate the danger of an insider threat by requiring all users and devices attempting to access the network to verify their identity. Zero knowledge proofs uses the blockchain to protect data transmitted over the Internet. Utilization of these new technologies will protect your company's data and your board members and C-suite executives from potential liability.

There are also low tech solutions that board members and executives should be aware of and implement to protect their company from a data breach. These solutions include having a vigilant IT department that actively monitors the status of the company's computer network, and board members and executives having regular communications with those IT professionals regarding potential threats to the network. There have been cases brought against board members and company officers for violating their fiduciary duties for failing to take these simple steps. Board members and executives should regularly meet with the company's IT department or vendors, and discuss potential threats to the company's network and what reasonable steps need to be taken to protect the personal information the company collects from its customers and employees. Simply being proactive and actively involved in protecting against a data breach or cyberattack is one of the primary ways for board members and C-suite executives to avoid being found personally liable for a cyberattack or data breach. --- Alexander L. Turner

---

Two Biometric Identifiers are Better than One. Researchers Fuse Face, Ear Images

"Researchers in a multinational team say they have created a biometric recognition system that uses three-dimensional images of faces and ears together that is 99.25 percent accurate with an 0.75 percent error rate threshold."

Why this is important: Two-factor authentication is coming for your face! By fusing biometric data sets of facial and ear scans, researchers have developed a system touting 99.25 percent accuracy. The general concept is that a 3D image using a blend of principal component analysis for the face, and independent component analysis for the ear, can yield a much more secure and accurate biometric identifier. This opens several new avenues for improving biometric security. The more accurate a biometric identifier is, the harder it is to breach. But other practical challenges such as large file size, additional computing power, and convenience still loom. Companies seeking to build independent data sets for biometric identifiers also will need to focus attention on the heavy costs, and legal risks, associated with additional storage and encryption. Passwords can be changed. The human ear remains a stable identifier for many years, which raises the risk associated with a data breach. It remains to be seen whether two heads are actually better than one, but these techniques and findings are promising. **---** Brian H. Richardson

---

NFT Sales Drop 92% Since September's High

"The reasons include the rising interest rates, which have put a squeeze on riskier bets in the financial markets, in which NFTs are some of the most speculative."

Why this is important: NFT sales have dropped about 92 percent since their peak at the end of 2021, and the average sale price is now less than one-third of its peak average. The number of active wallets for NFTs dropped about 88 percent since then as well, and Google Trends noted that searches have fallen roughly 80 percent since January. Even some of the best known NFTs are selling at a loss. Media claims the NFT market is dying; a recent WSJ article deck asked, "Is this the beginning of the end of NFTs?"

At the same time, NFT transactions have caused major blockchain crashes. Earlier this month, the ethereum blockchain suffered an overload during an NFT minting sale by the Bored Ape Yacht Club, which caused a drastic slowdown and unheard-of transaction fees up to $10,000. Also, this month the Solana blockchain crashed and was down for seven hours as bots overloaded it trying to win a limited edition NFT.

Despite the wary headlines, the drop in NFT sales and prices seems to align with what's going on in the world. Inflation, rising interest rates, international war, and a lingering pandemic are stressing financial markets. It certainly doesn't seem like the time for playful, risky investments. As investors heed more defensive positions, NFTs—one of the most speculative bets—are losing some steam. --- Alison M. Sacriponte

---

Facebook Doesn't Know What It Does with Your Data, or Where It Goes: Leaked Document

"'We do not have an adequate level of control and explainability over how our systems use data,' Facebook engineers say in leaked document."

Why this is important: Facebook has a tremendous amount of your personal data, including pictures, information about your preferences, political leanings, and who your family and friends are. The general public has no idea what Facebook does with all of that information. Scary thing is, neither does Facebook. With the rise of privacy regulations around the world, Facebook has the daunting task of complying with those regulations. What is permissible in the United States regarding the sharing or selling of personal data may not be allowed in the EU. The problem is that Facebook does not have "adequate levels of control or explainability over how its systems use data[,]" which makes it exceedingly difficult for Facebook to adhere to disparate regulations. The European Union's General Data Protection Regulation ("GDPR") requires that personal data can only be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes." If Facebook does not know what is happening to the data it is collecting, and how it is being used, then it cannot be in compliance with the GDPR, opening Facebook up to considerable liability.

The U.S., on the other hand, does not have a universal federal privacy law that governs the collection and use of personal data similar to the GDPR. That is what makes international compliance difficult for Facebook. However, if Facebook is unable to comply with its own privacy notice that tells Facebook's users exactly what Facebook will and will not do with users' personal data, then it can become subject to FTC regulatory action for unfair and deceptive trade practices. That is why it is important not only for your organization to have a privacy policy in place for how your organization plans to use personal information, but to have a privacy notice that tells your customers how their personal data will and will not be used. Once you have a privacy policy and have informed customers with a privacy notice, you must strictly comply with the policy and the contents of the notice. If you plan to use customers' personal data in a way different that outlined in your privacy plan and as conveyed to the customers in the privacy notice, then you must amend the privacy plan and obtain new approval from customers through an updated privacy notice. Failure to do so can result in FTC regulatory action. --- Alexander L. Turner

---

CDC Tracked Millions of Phones to See If Americans Followed COVID Lockdown Orders

"Newly released documents showed the CDC planned to use phone location data to monitor schools and churches, and wanted to use the data for many non-COVID-19 purposes, too."

Why this is important: This article reports on the fact that the CDC paid $420,000 to SafeGraph for one year of access to data. SafeGraph calls itself a data company, but others describe it as a data broker. In this case, the CDC purchased access to location data on tens of millions of mobile devices in the U.S. for the stated purpose of performing analysis of compliance with curfews imposed as a result of COVID-19. However, a FOIA request to the CDC discovered that it also had identified a list of use cases for the data, and many of the use cases had nothing to do with COVID-19, including examining "the effectiveness of public policy on [the] Navajo Nation" and tracking current "patterns of those visiting K-12 schools and compar[ing that data] to 2019." The FOIA request also discovered that the CDC intends to use the data to monitor "travel to parks and green spaces, physical activity and mode of travel, and population migration before, during, and after natural disasters." Privacy advocates have been expressing concerns over contact tracing and vaccine passports being used as tracking and surveillance tools. This move by the CDC is sure to fan those flames. --- Nicholas P. Mooney II

Many CEOs are Using These Ridiculously Simple Passwords, Cybersecurity Report Shows

"New research by NordPass, a password manager, and independent researchers has revealed that passwords such as '123456,' '12345,' 'password,' '123456789,' and 'qwerty' are among the most hacked passwords used by CEOs."

Why this is important: As discussed above, C-suite executives, including the CEO, have a fiduciary duty to reasonably protect the company against cyberattacks and data breaches. The problem is, a recent study found that a significant number of the world's CEO and business owners have incredibly weak computer passwords. These simplistic passwords endanger the company's entire computer network. In fact, 80 percent of data breaches are the result of easy-to-crack passwords. So before your company invests in expensive quantum computing and encryption, the first step to cyber security is the reasonable and simple step of having everyone at the company, including the CEO or owner, having robust and unique system passwords. By taking this simple step, you can eliminate a significant threat to your computer network. --- Alexander L. Turner

---

California Pizza Kitchen Class Action Claims Company Failed to Protect Workers' Private Data from Breach

"California Pizza Kitchen has agreed to pay $3.7 million to resolve claims it failed to protect its workers' private data from a data breach last year."

Why this is important: Data breaches can extend beyond consumer information as is the case with California Pizza Kitchen. Employees of the California Pizza Kitchen allege that a data breach exposed the social security numbers of current and former employees. It is alleged that the scope of the breach is more than 100,000 individuals. A class action lawsuit was filed against the employer in December 2021 on the basis that the company failed to properly secure the employees' personal information that was exposed after a cyberattack. The California Pizza Kitchen has agreed to pay $3.7 million to resolve the claims.

As part of their routine business processes, employers store personal information. How employers maintain such information is crucial to prevent its' exposure. Employers must be aware of the types of data, how it is secured and whether the precautionary measures will be sufficient to withstand a breach. Although an organization may incur costs to conduct such a review, a proactive approach is less costly than responding to the exposure of personal data. --- Annmarie Kaiser Robey

---

The First Commercial Brain-Computer Interface is Starting Human Trials

"The company developing the interface, Synchron Inc., is a competitor of Elon Musk's Neuralink Corp. Synchron Inc. beginning clinicals puts the company on a path toward mainstreaming controversial technology that could have wider use in helping people overcome disabilities and paralysis."

Why this is important: Enrollment is officially underway in the Stentrode brain-machine interface clinical trial! Synchron, Inc. has announced that the first of six proposed human trial subjects is enrolled in its long-term feasibility study. The initial focus of this NIH-funded trial is on patients with paralysis. This trial is unique in that it seeks approval for long-term use outside the lab setting, making it an apparent first of its kind. Where the focus of much of the past brain-stimulation research has required implants surgically placed directly in the brain, such as with deep brain stimulation technology, the Stentrode device is different because it reaches the brain through the blood vessels. Once there, the device translates brain activity into signals used for controlling an external digital device. This would allow for texting, email communication, or even going online! Efficacy trials will need to follow, but this is a very big step for the development of brain-machine interface technology. There are many applications for this type of device beyond treating paralysis. If successful, this trial could open the door for other companies to explore those wider applications, and seek regulatory approval. Companies with an interest in brain-machine interface technologies should follow this trial closely. --- Brian H. Richardson

---

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