SHARE:

Join Our Email List

View as Webpage

April 14, 2022

Welcome

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

The Pennsylvania Bar Association is hosting their Civil Litigation Section Annual Retreat on April 29-May 1 in Gettysburg, PA. We are a sponsor and will be in attendance. We would love to see you there. Click here to learn more.

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*

Britain Announces Plans to Mint Its Own NFT as It Looks to ‘Lead the Way’ in Crypto

"Glen said the government was also 'widening' its gaze to look at other aspects of crypto, including so-called Web3, a movement that proposes a more decentralized version of the internet built on blockchain technology."

Why this is important: The Royal Mint has been tasked with creating and issuing the U.K. government’s first official NFT. This announcement would appear to be a well-timed PR move to bring attention to the push to make the U.K. a leader in the field of crypto. City Minister John Glen outlaid a number of key points in the plan to accomplish this goal during a London fintech event; key among which is the focus on bringing so-called stablecoins (a type of cryptocoin that derives value from sovereign currencies) into existing electronic payment regulations. These announcements and outlines come at a time that other governments are also pushing focus towards embracing crypto and beginning to regulate in the field, with many taking tentative first steps into a field where the impacts of broadranging regulation is simply unknown. With the U.K. now firmly declaring its intent to become a world crypto-hub, and beginning to layout actual steps to achieve this goal, pressure will be on the U.S. and other countries to double-down on their own such efforts. --- Brandon M. Hartman

Privacy Breach Claim Against Employer Needs Story of Unreasonable Behavior

"The decision here is simple, the plaintiffs sued WM for a data breach, but failed to allege that any of WM's actions were unreasonable."

Why this is important: You would not think that something as low tech as picking up garbage would be at risk of a data breach. Unfortunately for WM, one of the country's largest garbage collection companies, it discovered that its servers had been breached and the PII of thousands of current and past employees had been compromised. WM's current and past employees brought a class action against WM for negligence, breach of implied contract, breach of fiduciary duty, and unjust enrichment. However, the S.D.N.Y. dismissed the action because the putative class failed to plead facts that showed that WM's actions in protecting its employees' PII were unreasonable. This is significant because when an entity handles or maintains PII it does not have to make every effort possible to absolutely protect that information from all cyberattacks, it is only required to make a reasonable effort to protect that information. What this means is that an entity that is the victim of a data breach is not strictly liable to the owners of the PII it maintains. This case is another one in recent history that shows that just because your company is the victim of a cyberattack or data breach, that does not necessarily mean that you are liable to the owners of the PII you maintain as a result of that attack. --- Alexander L. Turner

Task Force, Commission Want Government Intervention with AI; Especially Facial Recognition

"A task force created by University of Pittsburgh, for instance, has published a report examining the use of AI algorithms, including those behind facial recognition systems, in its home city and county, Allegheny."

Why this is important: Public algorithms are a potentially invaluable tool to local governments that also pose a potent threat. In the Pittsburgh region (where the study cited in the article occurred), public algorithms are used in "child welfare investigations, bail determinations, and a variety of other public functions." Yet, while these often significant decisions are based upon data from a vast reservoir of information, the public is largely in the dark about where the information is coming from, how the algorithms work, and why they are being used. Moreover, many of the "public" algorithms have little public input in their implementation, or little public accessibility about how information is being harnessed and used. This is especially problematic, given that the study explicitly recommended against the use of facial recognition systems at this time. The study highlighted how facial recognition systems were "plagued with errors," often fed implicitly biased data by the algorithms, and had a high potential for harm due to their use in high-risk situations (i.e., issuance of an arrest warrant for a suspected criminal). The study emphasizes and underlies the need for greater transparency and public input into how public algorithms are implemented by the governments seeking to use them. These algorithms are a potentially valuable tool in improving the health and welfare of communities when used in a proper manner. --- Alyssa M. Zottola

Class Action Challenges PetSmart's Use of Voice Recognition Tech

"PetSmart required warehouses workers to use the technology to create an individual voiceprint, unique to each person, the complaint alleged."

Why this is important: This article reports on another lawsuit brought under Illinois's Biometric Information Privacy Act ("BIPA"). This one targets how PetSmart collected, maintained, and used employees' voiceprints. The lawsuit alleges that PetSmart required warehouse workers to use technology to create an individual voiceprint that was then used to interact with a central computer to carry out their work functions. The lawsuit alleges that PetSmart failed to obtain workers' consent to collect their voiceprints, failed to advise them of the purpose for which they were collected, failed to warn them of the length of time in which they would be stored and used, and failed to timely destroy them. BIPA has real teeth. In addition to providing for a private right of action, it permits plaintiffs to recover penalties of $5,000 for intentional violations. It isn't the only state statute that addresses biometric privacy. We've repeatedly reported in *Decoded* on new lawsuits brought under BIPA or a similar statute. With the number of these lawsuits on the rise, employers need to pay particular attention to the ways in which they might be collecting, maintaining, and using information that falls under these statutes. --- Nicholas P. Mooney II

After Decades, Researchers Deliver First Complete Human Genome Using Long-Read DNA Sequencers

"According to researchers at the Telomere to Telomere Consortium and the National Human Genome Research Institute, revealing the final unknown corners of the genome will open up new studies into how chromosomes properly divide and research on more than 2 million additional genetic variants."

Why this is important: Many think that we already completed analysis of the human genome. We did, minus a few holes we had to fill in; holes amounting to 8 percent! That limited use of the information for DNA research and drug development. Now, with all the holes filled, researchers may broaden the development of treatments and drugs. --- Hugh B. Wellons

NFTs are a Privacy and Security Nightmare

"The blockchain isn't as 'anonymous' as you might think."

Why this is important: Do you want everyone to know every financial transaction you make? If you do, then cryptocurrency and NFTs are for you. Crypto and NFTs use public blockchains to provide necessary transparency to maintain accurate records, and none of those transactions are private. With crypto, there are ways to circumvent everyone knowing about your financial transactions, like not tying your name or address to your crypto wallet, or using a unique crypto wallet for each transaction. However, this is not possible with NFTs because they are fundamentally unique, identifiable tokens. If you tie your NFT to any part of your online identity, then it is super easy for anyone to know what other transactions you have made with your wallet. Maybe having everyone know that you like to buy cute cat emoji NFTs is no big deal, but problems arise with the push to use NFTs for home ownership, medical records, and social media. The result is that significant portions of your life are no longer private and cannot be deleted from the blockchain. Moreover, NFT platforms lack basic security features. Because your wallet is now publicly known, anyone can put NFT spam in your wallet without requiring you to approve it. When you discover that your wallet is cluttered with all of this NFT spam, you cannot just delete it, but you need to pay to have it removed. While your life may be an open book, and you want to be on the cutting edge of financial technology, you need to be aware of the security risks that go along with playing in the NFT sandbox. --- Alexander L. Turner

How Cryptocurrency Exchanges can Improve User Authentication

"Studies have found that 56% of exchanges worldwide have no KYC solutions in place."

Why this is important: While cryptocurrency booms and matures, security concerns abound. As the infrastructure grows, so do the opportunities for bad actors and illicit activity. 2021 was a record-breaking year for such crime -- fraudsters stole more than $14 billion in cryptocurrency. Cryptocurrency exchanges are aware of these risks, but many of their security measures have proven ineffective. Moreover, studies show that 56 percent of exchanges worldwide have no KYC solutions in place. Document verification is one common method for onboarding users, but it is vulnerable to fake IDs and can impede the onboarding process for customers who may never even transact. Many users hold cryptocurrency as an investment rather than transacting with it, while the risk of malfeasance naturally occurs as funds are moved around. One improvement could be to move the document verification step to the time of purchase instead of at sign-up. Exchanges also can streamline and improve the document verification process with technology such as algorithmic name and date-of-birth matching, and biometrics such as face and fingerprint scans. These applications can automate the process and improve accuracy, allowing exchanges to better ensure the veracity of their customers. Better user authentication could greatly improve cybersecurity, and, as cyber criminals employ new methodologies, it's pertinent that exchanges keep up with due diligence to protect the integrity of this ecosystem and the trillions of dollars it holds. --- Alison M. Sacriponte

Biotechnology's Vital Role for Efficient and Sustainable Water Purification

"Advanced biotechnology allows for biological solutions to traditional water and waste-treatment challenges such as sludge management, degradation of recalcitrant compounds and biogas generation."

Why this is important: Yes, biotech is used in water and waste treatment too! This article introduces you to how biotech developments make water and waste treatment safer and more efficient. It is a bit technical, but it explains how important new developments are to ridding water and waste of dangerous compounds. --- Hugh B. Wellons

Physical Infrastructure Cybersecurity: A Growing Problem for Data Centers

"Data centers remain vulnerable to attacks against operational technology – and broader adoption of IoT isn't helping."

Why this is important: It is not just the data held in data centers that are being hacked, but the physical components of the data centers themselves that are vulnerable to attack. Cyberattackers do not just want to steal your data, they may want to destroy it in order to create chaos in your organization. They do this by gaining access to the data center's physical systems through the data center's physical hardware like HVAC controllers, security badge readers, and IP cameras. These systems are often overlooked as cybersecurity threats. Something as simple as disrupting the cooling system for the servers could result in the servers overheating and the data they maintain being corrupted. Another avenue of attack are wipers. These cyberattacks utilize the data center's hardware vulnerabilities to gain access and look like a ransomware attack. However, when the ransom is paid, instead of returning the data, the wiper erases it. All physical systems should be evaluated for their need to be connected to the Internet, and if they do not need to be connected to the Internet, then they should be disconnected. But some systems cannot be disconnected, like HVAC or security systems. In those cases, the data center should work with its third party vendors to ensure the security of these systems. Failure to do so could be catastrophic. With cyberattacks on data centers on the rise, infrastructure security at data centers is critical. When evaluating which data centers you choose to store your organization's data, the data center's physical components and cybersecurity of those physical components should be an integral part of your evaluation. --- Alexander L. Turner

Senators Drill Down on Rising User Fees, Cybersecurity and Clinical Trial Diversity in MDUFA Hearing and FDA Asks Congress for 14% Bump in Device Budget for Supply Chain, Cybersecurity Programs

"While Tuesday's hearing did not include FDA officials, senators questioned industry groups as they consider an increase in the amount the agency can collect in fees from device makers."

"After seeing user fee funding climb 75% from 2019 to 2021, FDA is now facing its second year of minimal growth in the money it receives from industry."

Why this is important: Two articles from the same source discuss typical (and specific) funding issues for biotech. Issues as broad as cybersecurity and clinical trial diversity drive FDA funding, as it is asked to do more in less time. Amongst all that, the FDA is negotiating its fifth Medical Device User Fee

Amendments agreement. This agreement sets the user fees and standards for FDA review of medical devices. It is a primary funding source for that portion of the FDA effort. Senators reviewing this are concerned about added cost to patients. Still, while use of medical devices is increasing rapidly, the FDA is receiving only small additional amounts from industry. The FDA also needs additional funding to deal with cybersecurity concerns in medical devices. These two articles demonstrate that our amazing acceleration of development in the life sciences comes at a price. The regulatory arm that evaluates these new products is asked to do more, more quickly. --- Hugh B. Wellons

FTC Rules by Enforcement in Privacy, but for How Long?

"The agency has brought 20 different cases related to privacy in the last two years."

Why this is important: This article reports on the recent efforts by the FTC to fill in the gap left by the lack of a federal law addressing data privacy. While states have enacted data privacy laws, there is not yet an overarching federal data privacy law. The FTC has stepped into the void by "regulating by enforcement," meaning that it has filed enforcement lawsuits against alleged violators. It typically brings those lawsuits under Section 5 of the Federal Trade Commission Act, which mirrors state and federal UDAP statutes in prohibiting "unfair or deceptive acts or practices in or affecting commerce." The lawsuits then serve as a warning and guideline to others that the FTC views certain activity as violating the FTC Act. Until there is regulation at the federal level, we expect agencies like the FTC to continue to regulate by enforcement. --- Nicholas P. Mooney II

The Future of NFTs Lies with the Courts

"As the first cases involving NFTs hit the dockets, courts will decide questions around ownership, art, and commerce."

Why this is important: The world of crypto is, as all emerging e-ideas and technologies eventually do, running headlong into the realization that the laws of the real world do indeed apply to cyberspace. The key issue here, as has been brought up at multiple points in the discussion of NFTs and legal rights, is ownership of the copyright to a particular work on which a given NFT is based. Several cases outlined here turn simply on this mistaken belief that creation, sale, and ownership of an NFT somehow confers copyright rights in the underlying work to NFT owner; this is simply not the case. However, the pending case of *Hermès v. Rothschild* is a much more fundamental issue of how digital art can be analogized to traditional art and long-standing legal concepts and traditions as to expression. In short, the artist Mason Rothschild is making digital versions of Hermès' Birkin handbags in which he asserts that the digital handbags, dubbed "MetaBirkins," are pixelized to appear furry so as to highlight his views of the animal cruelty inherent in producing the actual handbags. Hermès does not produce or sell its own NFTs, so its claim is based on consumer confusion and dilution of the brand. This article compares the scenario at play here to Andy Warhol's famous Campbell's Soup Cans painting, with digital art subbing in for "traditional" art techniques. Turning on both issues of copyright and First Amendment, this will certainly be a fascinating and important case to watch play out. --- Brandon M. Hartman

Apple Warning: 'HUGE AirPods Security Flaw' Could Leak Your Private Info to Strangers

"Some used AirPods reportedly stay linked to the previous owner's iCloud account despite a factory reset."

Why this is important: Your old AirPods are a major security threat to your iCloud. It was recently discovered that 80 percent of AirPods returned to Walmart remain connected to the original user's iCloud. Even after they are reset by the reconditioning company, some new purchasers have found that returned AirPods remain tethered to the original owner's iPhone, thereby creating the potential risk of a data breach of the original owner's iCloud. Experts attribute this problem to Apple's strategy to have all of its products synchronize with each other and not be "return friendly." Who knew that your earphones were going to betray you and be another avenue of attack for cybercriminals. --- Alexander L. Turner

Software Vulnerabilities Point to Need for ICS Security in Healthcare

"Industrial control system (ICS) security requires defense in depth measures and regular vulnerability patching."

Why this is important: You probably know already that cybersecurity is a problem in almost every aspect of life, but it particularly affects biotechnology. Of course, the thought of someone hacking a medical device is scary. It also is scary that certain countries promote hacking of development records, providing proprietary information to developers in the hacking country. In addition, hacking and sharing personal health data is epidemic. The Cybersecurity and Infrastructure Security Agency, using National Institute of Standards and Technology data and recommendations, issued a new advisory about a compromised patient portal. I think that the key takeaway is that the current standard in biotech operations should include an industrial control system at least as tight as commonly used in such companies. We aren't in Kansas anymore. --- Hugh B. Wellons

---

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