SHARE:

Join Our Email List

View as Webpage

August 31, 2022

Welcome

Welcome to the 17th issue of *Decoded* for the year.

We are pleased to announce that 60 of the firm's attorneys were selected by their peers for inclusion on the 2023 Best Lawyers list, 10 were selected as Best Lawyers "Lawyers of the Year," and nine others were selected as Best Lawyers "Ones to Watch."

Recognition by Best Lawyers is based entirely on peer review. Its methodology is designed to capture the consensus opinion of leading lawyers about the professional abilities of their colleagues within the same geographical area and legal practice area. You can learn more by clicking here.

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

---

CFPB Takes Action to Protect the Public from Shoddy Data Security Practices

"The bureau said the circular does not suggest that particular security practices are specifically required under the Consumer Financial Protection Act."

Why this is important: The Consumer Financial Protection Bureau ("CFPB") recently jumped into the data security pool. Pursuant to a circular published by the CFPB, financial companies may be in violation

of the Consumer Financial Protection Act ("CFPA") if they fail to take adequate measures to safeguard consumers' data. While the CFPB did not specifically require any particular actions financial companies need to take to protect consumers' data, it did offer a few suggested actions. These suggested actions included the implementation of multi-factor authentication, adequate password management, and timely software updates. The CFPB went on to state that a financial company's failure to implement these simple suggestions could trigger liability under the CFPA. --- Alexander L. Turner

---

NFTs Turn Out to be a Great Channel of Revenue for Businesses, Ask Nike

"Call it FOMO or just a passing fad, but businesses like Nike, Dolce & Gabbana, Tiffany, Gucci, and Adidas are reaping millions from NFTs."

Why this is important: This article discusses the success several fashion brands are enjoying with minting and selling non-fungible tokens ("NFTs"). Nike is leading the pack with $185 million in revenue from NFT sales. The article discusses a critical piece of Nike's NFT strategy, its acquisition of RTFKT, the company that is creating most of Nike's NFT collections. The point to be taken from this article is a well-planned NFT strategy can not only build deeper relationships with customers but also can lead to big revenue. **---** Nicholas P. Mooney II

IRS Can be Sued for Unlawful Data-Collection in Violation of the Fourth and Fifth Amendments

JAMES HARPER v. CHARLES P. RETTIG, in his official capacity as Commissioner of the Internal Revenue Service

Why this is important: Does sovereign immunity protect the IRS from suits alleging that the IRS engaged in unlawful collection of citizens' financial data? In *Harper v. Rettig*, the First Circuit said no, sovereign immunity does not protect the IRS from these types of suits. In *Harper*, the IRS, in search of tax evaders, allegedly improperly obtained the financial information of Mr. Harper and thousands of other cryptocurrency traders in an information gathering operation targeting third-party cryptocurrency exchanges Abra and Coinbase. The investigation was not based on any reasonable suspicion of wrongdoing, but appears to have been a fishing expedition. The IRS went to Abra and Coinbase to gather information regarding traders' cryptocurrency transactions without a warrant or a subpoena. Instead, the IRS issued a third-party summons to the exchanges for the information. The subjects of this investigation, including Mr. Harper, were not provided with pre-data-collection notices or an opportunity to contest the IRS's requests for the information. Once the IRS obtained information regarding Mr. Harper's transactions from the exchanges, the IRS informed Mr. Harper that he was subject to an enforcement action related to those transactions. In response, Mr. Harper sued the IRS and 10 unidentified agents alleging that the IRS and its agents violated his Fourth and Fifth Amendment rights, as well as violating 26 U.S.C. § 7609(f), by acquiring Mr. Harper's personal financial information from Abra and Coinbase through the third-party summons process. Mr. Harper alleged that he had an ownership interest, and a reasonable expectation of privacy in the financial information Abra and Coinbase held related to his accounts. Mr. Harper sought damages and declaratory and injunctive relief, including an order requiring the IRS to expunge his financial information from its records.

The IRS filed a Motion to Dismiss all of Mr. Harper's claims, including his claims for declaratory and injunctive relief. The district court agreed and dismissed Mr. Harper's claims for monetary damages, and declaratory and injunctive relief. The basis for the dismissal of Mr. Harper's request for injunctive relief, and the only ruling he appealed, was a lack of subject matter jurisdiction because the district court held that the Anti-Injunction Act of the Internal Revenue Code was an exception to the Administrative Procedure Act's waiver of sovereign immunity. However, on appeal, the First Circuit reversed the district court's ruling based on the recent Supreme Court decision in *CIC Services, LLC v. IRS*, a ruling that came out after the district court's decision. *CIC* held that the Anti-Injunction Act ("AIA") does not prohibit a suit "seeking to set aside an information-reporting requirement that is backed by both civil tax penalties and criminal penalties." Accordingly, because Mr. Harper's suit sought to set aside the IRS's alleged illegal information gathering and was not a suit brought to enjoin a tax's assessment or collection, the First Circuit held that Mr. Harper's suit was not subject to the AIA's limits on court jurisdiction. Specifically, the First Circuit noted that *CIC* defined information gathering as a "phase of tax administration procedure that occurs before assessment [or] collection." Therefore, the First Circuit held that because the IRS's

actions against Mr. Harper "clearly fall within the category of information gathering" therefore "the [AIA] is not an applicable exception to the United States' waiver of sovereign immunity." As a result of this decision, the district court now has subject matter jurisdiction to decide whether the IRS's actions in obtaining Mr. Harper's trading information from Abra and Coinbase through a third-party summons violated Mr. Harper's Fourth and Fifth Amendment rights, as well as 26 U.S.C. § 7609(f). --- Alexander L. Turner

---

FTC Weighs Sweeping New Rules on 'Commercial Surveillance' and Big Data

"The Federal Trade Commission is considering whether to write sweeping new regulations that could restrict how businesses collect and use consumer data, hinting at a possible crackdown on commercial algorithms and a sprawling economy powered by the personal information of millions of Americans."

Why this is important: Earlier this month, the Federal Trade Commission ("FTC") issued an advance notice of proposed rulemaking seeking public comments on harms suffered by consumers from the prevalence of commercial surveillance and corporate data security practices. Depending on the comments received, the FTC will decide whether to implement new rules and regulations to address how companies "collect, aggregate, protect, use, analyze, and retain consumer data, as well as transfer, share, sell, or otherwise monetize that data." The FTC is hopeful to receive comments that will specifically guide regulations targeted at unfair or deceptive practices. The public comment period has opened, and the deadline for submitting comments is October 21, 2022. In addition, a virtual public forum will be held on the afternoon of September 8, 2022. Responding to an ANPR is an important opportunity for concerned members of the public, including businesses, to shape the regulations that will impact their business practices going forward. As the risks associated with data breaches continue to rise, and expand across a wider variety of industries, the laws and regulations must keep pace with the need for adequate protections for consumers. Critics of the proposed actions take the position that such sweeping regulation as what the FTC is considering should be addressed by the Legislature, and not the FTC. Measures are certainly being proposed and advancing in Congress as well, and interested parties with concerns for data privacy regulation should weigh those proposals and comment to ensure their perspective is considered. --- Brian H. Richardson

---

Smartphone-Linked Blood Pressure Monitors Fail to Beat Traditional Devices, Study Finds

"The trial, which mostly enrolled people who were relatively comfortable using technology, failed to meet most of its secondary endpoints, including one that looked at patient satisfaction."

Why this is important: As more people rely on smartphones for their daily activities, the healthcare industry has created apps to facilitate the monitoring and improvement of physical health. Companies such as Hello Heart and Livongo offer hypertension management plans that are connected to blood pressure monitors. Such apps provide convenient access for individuals comfortable using technology. However, this does not mean that the programs are necessarily more effective than traditional monitors. The National Patient-Centered Clinical Research Network conducted a randomized study to compare the standard at-home blood pressure monitor and a smartphone-linked device with an associated app. The researchers concluded that although there was a decrease in systolic blood pressure with the smartphone device, it was not better than a traditional monitor.

When determining the best method for managing blood pressure, it comes down to personal preference. Some people feel most comfortable using an at-home monitor. Others may like the convenience of having the information accessible on the phone. As with any health improvement plan, it is best to consult with your physician and choose the path that will lead to you long-term improvements that can be sustained over time. --- Annmarie Kaiser Robey

---

Third-Party Attacks Spike as Attackers Target Software Connections

"When an attack on one organization becomes a window for potential attacks on many, threat actors take notice and circle back for more."

Why this is important: Cyberattackers "are people and people like to find shortcuts to maximize their reward for the minimum amount of effort." This thought explains some of the recent third-party attacks. Instead of executing a frontal assault on secure companies, many threat actors (the buzzword used for people who commit cyberattacks) are finding success in attacking third-parties in the companies' supply chains. This can lead to a double recovery. First, the threat actor may be able to ransom the third party for the release of its data. Second, the threat actor may obtain data that gives her/him a key into the original company's systems. The message here is clear: companies need to not only take steps to secure their own systems but also be mindful of the security steps taken by vendors and others in their supply chain. **---** Nicholas P. Mooney II

Surprise! Senior Living Operator's Insurance Doesn't Cover Class Action Biometrics Suit

"Church Mutual argued in a complaint that its policies with Prairie did not cover 'wrongful employment practices,' including 'invasion of privacy.'"

Why this is important: We here at *Decoded* repeatedly tell you that you need sufficient insurance coverage to guard against data privacy issues. But you not only have to make sure that you have a sufficient amount of coverage, you also have to make sure that the coverage you do buy covers all possible data privacy issues. Prairie Valley Supported Living found out the hard way that not all insurance coverage is the same. It thought that it had sufficient coverage to defend against a class action lawsuit brought by employees related to the facility's alleged violation of Illinois' Biometric Information Privacy Act. The employees allege that the facility's collection, use, and dissemination of biometric identifiers violated the Act. However, its insurer, Church Mutual Insurance Co. of Wisconsin, brought a declaratory judgment action that it does not have to provide Prairie Valley with a defense under the policy because the policy did not cover wrongful employment practices, including invasion of privacy. Because the putative class action plaintiffs alleged that Prairie Valley required them to clock in and out using their fingerprint without first requiring them to sign a waiver or getting their permission to collect their biometric data as required by the Act, Church Mutual denied coverage because this was a wrongful employment practice that invaded Prairie Valley's employees' privacy. The Court agreed and held that Church Mutual had no obligation to provide a defense or indemnify Prairie Valley in this case. This is a cautionary tale about clearly defining what is included in your data privacy coverage and what is not when you purchase the policy so that you are not surprised later. --- Alexander L. Turner

---

Risk of Cyberattack Emerges as Top Concern of US Executives

"The study shows 40% of top business executives consider cyberattack risk their top concern, followed by talent acquisition at 38%."

Why this is important: This article reports on a recent survey of 722 cross-sector U.S. executives regarding current attitudes toward cybersecurity risks. As the headline notes, 40 percent of those surveyed said that the risk of a cyberattack is their top concern. This response was not limited to chief information security officers ("CISOs"). Concerns about cybersecurity have bled into all C-suite offices and corporate boards. Almost half of those surveyed noted that they are making additional investments into their companies' cybersecurity defenses. We've reached a point where companies understand that cyber risks are more than merely an IT problem. Instead, they implicate serious risks to companies in terms of both financial losses and reputational harm. Add to this the fact that regulators at the federal and state levels have proposed regulations that would require more prompt and detailed disclosure of cyber incidents. These factors all lead to the recognition that cybersecurity is a concern for all corporate officers (not just the CISO) as well as board members. --- Nicholas P. Mooney II
