SHARE:

Join Our Email List

View as Webpage

September 15, 2022

Welcome

Welcome to the 18th issue of *Decoded* for the year.

We would like to take a moment and introduce you to several new additions to the firm.

Charles W. "C. W." Pace, Jr., recently joined the law firm as a partner in our Charleston office. C. W.'s primary areas of practice are estate planning, probate, commercial transactions, corporate law, and tax. He regularly provides advice and assistance to clients on a wide array of estate planning strategies, including various forms of complex transfer tax planning strategies, business succession, special needs trusts, and charitable trusts. He also advises fiduciaries on trust, probate, and estate matters.

Grace K. Dague joined the firm's Charleston office. A recent graduate of West Virginia University College of Law, her application with the West Virginia State Bar currently is pending. Once admitted to the Bar, her primary areas of practice will be corporate, technology and real estate law.

James W. McCauley Jr. joined our Roanoke office. A graduate of Widener Commonwealth Law School, he recently earned his Master of Laws degree from the University of Florida Levin College of Law. His application with the Virginia State Bar is pending. Once admitted to the Bar, his focus areas will be corporate law and trusts and estates matters.

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

IRS Says It Exposed Some Confidential Taxpayer Data on Website

"Tax agency says error led to posting about some taxpayers with IRAs."

Why this is important: In the last issue of *Decoded*, we discussed the fact that the IRS can be sued for violating taxpayers' Fourth Amendment rights when it engages in fishing expeditions in an attempt to identify tax evaders. In this issue, we discuss a recent self-inflicted data breach where the IRS posted the confidential information of approximately 120,000 taxpayers. The IRS published information from these taxpayers' Form 990-T, which is used by individuals with retirement accounts that earn business income within those retirement plans. The disclosures included names, contact information and financial information about the income within those retirement accounts. The IRS stated that the disclosure may be the result of a coding error related to charities' use of Form 990-T for unrelated business income. The coding error was due to the fact that Form 990-T filed by individuals are confidential, while charities' filings are public.

Do the affected taxpayers have the ability to bring a lawsuit against the IRS related to its publication of their personally identifiable information ("PII")? They may have a cause of action under the Privacy Act of 1975, which establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. Specifically, the Privacy Act prohibits the disclosure of confidential information held by the federal government without written consent. "Whenever any agency . . . fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual . . . the individual may bring a civil action." 5 U.S.C. § 552a(g)(1)(D). In a suit for damages under subsection (g)(1)(D), an individual has the burden of proving that: (1) the information at issue is covered by the Privacy Act's provisions; (2) the agency violated a provision of the Privacy Act not covered by the other civil remedies provisions; (3) the violation had an "adverse effect" on the plaintiff that was a "causal nexus" between the violation and the adverse effect; and (4) the violation was "willful or intentional." See, e.g., *Quinn v. Stone*, 978 F.2d 126, 131 (3d Cir. 1992); *Pierce v. Air Force*, 512 F.3d 184, 186 (5th Cir. 2007). However, a mere negligent or inadvertent violation of the Privacy Act is not enough to overcome the "intentional or willful" barrier for a plaintiff to maintain a Privacy Act claim against a federal agency. See, e.g., *Campbell v. SSA*, 446 F. App'x 477, 479, 481 (3d Cir. 2011). Consequently, even if the IRS's disclosure of PII had an "adverse effect" on these taxpayers, based on the facts stated in the article that the disclosure was the result of an inadvertent coding error, it is unlikely that these taxpayers have a sufficient basis to bring a Privacy Act claim against the IRS. --- Alexander L. Turner

FTC Sues Data Broker, Condemns Improper Data Privacy Practices

"The US Federal Trade Commission sued data broker Kochava over its alleged sale of geolocation data, signifying the Commission's commitment to cracking down on improper location and health data privacy practices after the fall of Roe v. Wade."

Why this is important: This article discusses the Federal Trade Commission's lawsuit against Kochava, an Idaho-based data marketing and analytics company. The suit relates to Kochava's collection, purchase, and sale of geolocation data from "hundreds of millions of mobile devices" for purposes of marketing and business analytics. The FTC alleges that, although this data may be anonymized, it can be linked to individuals and can trace them when they visit sensitive locations, like reproductive health clinics, domestic violence shelters, and places of worship. Kochava responded by filing a suit against the FTC and arguing that the FTC doesn't understand its business model. The parties seemed destined to fight this in court as the FTC has made clear it "is committed to using the full scope of its legal authorities to protect consumers' privacy." If you're interested in how anonymized data can be traced to identify you and then track you as you go about your day, read the December 19, 2019 article in *The New York Times* titled "Twelve Million Phones, One Dataset, Zero Privacy." --- Nicholas P. Mooney II

Sephora Hit by First CCPA Enforcement Action, Settlement Carries $1.2 Million in Penalties for Targeted Advertising

Privacy Violations

"The case involved third party access to information about customer purchases and the types of devices they were using, a privacy violation under the state's consumer law."

Why this is important: Sephora is being charged $1.2 million in penalties for violating the California Consumer Privacy Act ("CCPA"). An investigation by the Attorney General found that Sephora had not disclosed the fact that third parties were purchasing personal information about Sephora's consumers. Information that has been sold includes the types of items that customers were buying and, in some instances, information about the locations and devices that the purchases were made from. Sephora had been given 30 days to cure the issues with its privacy policy, but failed to do so. Sephora was one out of 112 businesses that had been found and notified about privacy violations, although most of the businesses changed their policies during the 30-day notice period. In the future, Sephora will be required to update its privacy policy and consumer disclosures to comply with the CCPA until it is replaced by the California Privacy Rights Act ("CPRA") in 2023. Businesses need to make sure that their privacy policies and consumer disclosures comply with the law prior to the CPRA becoming effective as the CPRA does not include the 30-day notice period for businesses whose policies do not comply with the law. --- Grace K. Dague

Growing Cyber Risks Add to Hospital Cost Squeeze, Fitch Cautions

"Cyber risk mitigation is becoming more expensive, but with hospitals' cost pressures mounting, spending on security may not be a priority, the ratings agency said."

Why this is important: We have discussed in previous issues of *Decoded* about the alarming increase in the number of healthcare related data breaches. In order to counter these increasing threats to patients' protected health information ("PHI"), healthcare facilities have to increase investment in data security. This includes an investment in hardware, software, and qualified personnel. Rating agencies are beginning to take notice of the increase in healthcare-related cyberthreats and the correlated rising costs in guarding against these attacks. The ratings agencies are concerned that rising expenses and decreasing profit margins are preventing healthcare facilities from properly addressing these increasing cyberthreats. The squeeze on profits that prevents increased investment in data security can result in a downward spiral in profitability, especially if it results in a data breach that impacts the quality of care and reputation of the facility. Another financial impact that the increased threat of a cyberattack has is that insurance premiums are increasing, making comprehensive coverage cost prohibitive. While these issues do not currently impact ratings scores, the rating agencies are aware that cyberthreats need to be taken into account in the future if the financial pressures and cyberattacks continue. --- Alexander L. Turner

Clash of the Titans: Moderna Sues Pfizer, BioNTech for mRNA Patent Infringement

"Pfizer and BioNTech have reeled in tens of billions of dollars with their world-leading COVID-19 vaccine Comirnaty, so a win for Moderna in either case could be quite lucrative."

Why this is important: This is not a surprise, rather just the preliminary salvo in a battle between the two similar technologies providing the mRNA vaccines. There is a reason that the Moderna and Pfizer vaccines have similar approval benchmarks, similar efficacy, similar, well, almost everything. Moderna claims that they got there first, and their patent is broad enough, so pay up or get out! BioNTech/Pfizer will claim the same. I expect this to settle, but the technology may be valuable enough to justify a long fight. It's also possible that it will motivate a merger or joint venture of some kind, although the antitrust laws may interfere. This technology might have better application in cancer drugs than in vaccines, so this will be interesting. --- Hugh B. Wellons

Charleston Receives Funding for LIFT Center Aimed at Green

Technology, Training and More

"The federal funding comes by way of the Appalachian Climate Technology Now Coalition of West Virginia, which the city is a member of along with Huntington, Logan, state universities and others."

Why this is important: Charleston will be receiving $13 million in federal funding through the Appalachian Climate Technology Now Coalition of West Virginia. The funding is going to be used to launch the Charleston Learning, Innovation, Food and Technology ("LIFT") Center in the manufacturing plant located on the East End of Charleston. The Lift Center will focus on the research and development of different innovative projects such as "electric batteries for clean vehicles, zero-emissions airplanes and renewable energy storage." The Lift Center also will include a training center for Coalfield Development jobs and a Refresh Appalachia food hub. The goals of this center will be important for transitioning West Virginia away from industries that have focused heavily on fossil fuels to more clean energy options. --- Grace K. Dague

US Sanctions Tornado Cash Over Ransomware Incidents, Worrying Crypto Privacy Advocates

"The sanctions are levied under the US Department of the Treasury's Office of Foreign Assets Control, which can order residents of the country to cease doing business with foreign organizations linked to terrorism or money laundering under penalty of steep fines."

Why this is important: Tornado Cash is an open-source cryptocurrency tumbler that helps crypto users maintain anonymity in transactions by sending cryptocurrency to Tornado Cash and later withdrawing cryptocurrency with a different address, thereby breaking the chain in the transactions. It has been used by threat actors in cyberattacks and ransomware heists, some of whom are linked to North Korea. That triggered the Department of Treasury's Office of Foreign Asset Control to take action. OFAC has the ability to order U.S. residents to cease doing business with foreign organizations linked to terrorism or money laundering. OFAC recently added Tornado Cash to the Specially Designated Nationals sanction list, which effectively stops any U.S. resident from doing business with Tornado Cash, even if their business is not in any way related to terrorism or money laundering. At bottom, this dispute implicates the extent to which computer code is protected speech and the limits, if there are any, to the government shutting down a business whenever it believes third parties are using it for illegal purposes. --- Nicholas P. Mooney II

A Cyberattack Hits the Los Angeles School District, Raising Alarm Across the Country

"The attack on the Los Angeles Unified School District sounded alarms across the country, from urgent talks with the White House and the National Security Council after the first signs of ransomware were discovered late Saturday night to mandated password changes for 540,000 students and 70,000 district employees."

Why this is important: Public school districts are now becoming targets of ransomware attacks. On September 3, 2022, the Los Angeles Unified School District ("LAUSD"), the largest in the country, was the victim of the latest ransomware attack against the nation's public schools. The size of the attack on the LAUSD resulted in urgent discussions with the White House and National Security Council. This is "consistent with the Biden administration's efforts to provide maximum assistance to critical industries affected by such breaches." It is reported that LAUSD followed the federal government's recommendations and it has not paid the ransom. In response to the attack, approximately 540,000 students and 70,000 district employees had to change their system passwords. Cyberattacks on school districts have increased since the beginning of the pandemic due to schools increased reliance on remote learning and other technology. This year alone, 26 school districts and 24 colleges have suffered ransomware attacks (see our discussion of the ransomware attack on Whitworth University below). 31 of these schools had data breaches resulting in student and employees' personally identifiable information released online. With school starting, the attacks are increasing at an alarming pace, with eight school districts having been hit since August 1, 2022. With the cost of ransomware attacks against large school districts being as high as $18,000,000, smaller school districts who are less able to afford the cost of

such attack must work closely with their IT and data security teams to fend off these attacks on their computer networks. --- Alexander L. Turner

Protecting Water from Cyberattacks

"The EPA faces different challenges than other agencies writing cybersecurity rules for the utilities they regulate because the U.S.'s water systems are so widely distributed and isolated."

Why this is important: This area is one of those that you may not think of when you think about cybersecurity. However, threat actors have targeted water supply systems in the past. In one of the more recent examples (which we covered in a prior issue of *Decoded*), a hacker broke into the computer network that ran the water system serving Oldsmar, Florida and changed the amount of sodium hydroxide in the water supply. These types of attacks do happen. The Environmental Protection Agency is working to stop them. It recently submitted its water security plan to Congress. The EPA also is expected to issue new rules later this year that require state officials to include cybersecurity in their inspections of water systems. The article notes one of the hurdles the EPA is facing in trying to create and implement a complete water cybersecurity plan: the U.S.'s water systems are distributed among approximately 148,000 different public water systems, some of which may not have the resources to develop and implement a complete and robust security plan. However, like the cybersecurity of connected medical devices, this area is one where lives literally can be at stake. We expect to see a push by the EPA and some members of Congress to make cybersecurity of water supply a priority. --- Nicholas P. Mooney II

Whitworth University Urges Patience After Data Breach, Reported Ransomware Attack: 'This Process Does Take Time'

"Describing the incident as 'a very sophisticated security issue involving our network systems,' Whitworth officials said in a statement to the campus community that they first became aware July 29 that the university's information systems had been infiltrated by 'outside actors.'"

Why this is important: Recently, Whitworth University in Washington state suffered a debilitating ransomware attack that crippled the University's network. It is currently unknown whether student, alumni, and/or employees' private information was stolen. Because there is not a universal data security law in the U.S, each educational institution should be familiar with the data security laws of the states where they provide services. The law in Washington State requires entities that collect and store personally identifiable information ("PII") to notify individuals whose information may have been breached within 30 days of the breach. If more than 500 Washington state residents must be notified of the breach of their PII, then the Washington Attorney General's Office must also be notified. There is an exception to the notification requirements "if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm." This is determined on a case by case basis. The U.S. Department of Education, through the Privacy Technical Assistance Center, provides a lot of information and tools to assist educational institutions with protecting their data against a cyberattack, including a Data Breach Response Checklist that an educational institution can use to help prevent a data breach and to help respond to a data breach.

Lockbit took responsibility for the attack on Whitworth University. Lockbit ransomware has become the "the most prominent threat in several sectors" in 2022 because, in addition to stealing information, LockBit uses online publicity to extort a ransom from the victim in order to unlock the victim's data. With LockBit being responsible for a third of all ransomware attacks, this is a known threat that educational institutions' IT departments and data privacy professionals should be aware of and working to counteract. Failure to put reasonable protections in place to prevent a known data security threat can result in liability for responsible IT department members and school administrators. --- Alexander L. Turner

Christian Dior Class Action Alleges Company Illegally Collects Biometric Data with Virtual Try-On Feature

"The Christian Dior Virtual Try-On feature works with facial recognition technology from a company called

FittingBox."

Why this is important: A class action lawsuit has been filed in Illinois federal court on the basis that the Christian Dior Virtual Try-On feature captures certain consumer biometric data without written consent. Various companies have incorporated similar features into their marketing plans as a way to facilitate a more personalized customer experience. In this particular case, the plaintiff utilized the feature to try on sunglasses. The Try-On program works with facial recognition technology. The plaintiff alleges that the Biometric Information Privacy Act was violated as she was not informed that her facial information would be captured and used. Other companies such as Estee Lauder have also faced litigation for their use and storage of biometric data.

As companies continue to develop clever features that allow the consumer to get a personalized view of their products, they must be mindful of the legal obligations related to the capture and storage of consumer data. A wise approach is to seek counsel and obtain a clear understanding of any disclosure requirements before implementing such tools. --- Annmarie Kaiser Robey

How Sandbox Programs Can Help Promote Innovation and Consumer Welfare

"Technological innovation is spurring startups and financial companies to make consumer transactions more accessible, faster and more affordable."

Why this is important: This article discusses how sandbox programs help promote innovation in consumer financial products and services. If you aren't familiar with sandbox programs, they are programs where technology companies are able to develop and experiment with new and innovative financial products and services with regulators temporarily pausing certain statutory and regulatory requirements that otherwise would apply. The thinking is, if those requirements applied, the companies behind the new products and services wouldn't be willing to test them if there's a possibility of violating the law and being held liable. By temporarily pausing the requirements (or making other allowances), the new products and services can be tested and possibly brought to market full-scale. These programs started in the U.K. in 2016 and have since expanded to many jurisdictions. There are 11 states in the U.S. with sandbox programs. As the article points out, enacting regulatory sandbox programs is an important tool in enabling innovation to bring more products and services (in other words, more choices for consumers) to market. However, the programs should be one part of an overall market-friendly regulatory scheme. --- Nicholas P. Mooney II

Financial Firms Liable for Consumer Financial Protection Violations with Lax Data Protection, Agency Warns

"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

CRISPR Method Boosts Efficiency and Yield Without Viral Vectors

"A newly developed CRISPR system, using single-stranded DNA HDR templates incorporating Cas9 target sequences achieved two- to threefold better knock-in efficiency and yield relative to dsDNA."

Why this is important: Many times before we have outlined the possible huge effects of gene editing through CRISPR Cas-9 gene manipulation. Now, researchers have treated a blood cancer, multiple myeloma, with a combination of this technology replacing one entire side of the double helix of DNA, substituting that "CRISPR'd" side for the old one. This also allows treatment with more efficiency, avoiding the broad use of viral vectors, which apply everywhere, instead of just where they are needed. This technology currently indicates best for cancer treatment, but it may be broader. --- Hugh B. Wellons