SHARE:

Join Our Email List

View as Webpage

October 13, 2022

Welcome

Welcome to the 20th issue of *Decoded* for the year.

We are pleased to sponsor the 2022 DRI Annual Meeting October 25-28 in Philadelphia. Join DRI to connect with the most influential civil defense attorneys and in-house counsel from across the country, expand your knowledge base with cutting-edge education, engage with our passionate legal community, celebrate past achievements and future goals with friends, and explore historic Philadelphia. Click here to learn more and register.

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

---

Cybersecurity Is Everyone's Responsibility

By: Nicholas P. Mooney II and Alexander L. Turner
as published in West Virginia Banker magazine, Fall 2022

A recent survey by PricewaterhouseCoopers revealed that U.S. executives now consider cyberattacks the number one risk their companies face. Concerns about cybersecurity have moved beyond the Chief Information Security Officer to the entire C-suite and corporate boards. Recent developments show executives are right to worry about those attacks because they can result in monetary loss, personal liability, and reputational risk.

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

Federal Appeals Court Ruling Means Class-Action Suits Over Data Breaches No Longer Require Proof of Actual Harm

"Earlier this month, the Third Circuit Court of Appeals' three-judge panel unanimously reinstated a putative class-action suit against a company that suffered a ransomware attack, leading to her sensitive information being released onto the dark web."

Why this is important: We have discussed in previous issues of *Decoded* that recent federal court rulings, including the Supreme Court's ruling in *TransUnion LLC v. Ramirez* and rulings in various federal circuits, including the Second Circuit, have tempered the risk in data breach lawsuits by requiring putative class members to plead that they have suffered an injury-in-fact in order to have standing to bring their claims. Recently, the Third Circuit has taken a unique position on what constitutes an injury-in-fact pursuant to the holding in *TransUnion*. The underlying case involved a suit by an employee who was required to provide her employer with a considerable amount of personal information, including her address, social security number, bank information, insurance and tax information, her passport, and information regarding her husband and child. In return for that information, her employment agreement provided that her employer would "take appropriate measures to protect the confidentiality and security" of her personal information. Despite this promise, her employer was a victim of a ransomware attack. Her employer informed its employees of the hack. Even though the plaintiff did not suffer any identity theft or fraud as a result of the cyberattack, she brought a putative class action on behalf of all of the company's employees against her employer for negligence, breach of contract, breach of fiduciary duty, and breach of confidence. Following the Supreme Court's holding in *Transunion*, the District Court dismissed the action for lack of standing because the putative class representative had failed to plead that she had suffered an injury-in-fact.

The putative class plaintiff appealed the District Court's opinion to the Third Circuit. The Third Circuit Court of Appeals found that the putative class plaintiff had standing, it vacated the District Court's ruling, and sent the case back to the District Court for consideration on the merits. To have standing to bring a case, a plaintiff must demonstrate that "he or she suffered an injury in fact that is concrete, particularized, and actual or imminent." In its ruling, the Third Circuit focused on the "imminent" part of that definition. Basing its decision on precedent of data breaches where there is a history of a future risk of injury following a data breach, the Third Circuit held that a substantial risk of future injury qualifies for standing to satisfy tine "imminent" language to sustain a finding of standing. This is especially true if the data breach is the result of an intentional act by a criminal hacking group. The Third Circuit went on to hold that an intangible injury like emotional distress related to being the victim of a data breach can count as being a "concrete" injury that supports standing. This decision makes it easier for plaintiffs to bring data breach cases in the Third Circuit, and bucks the trend of courts holding that fear of future identity theft following a data breach is insufficient to sustain a finding of standing. It also creates a split between the Circuits, which may result in the U.S. Supreme Court needing to weigh in again sometime in the future to further clarify what constitutes a basis for a finding of standing in data breach cases. --- Alexander L. Turner

---

Blueprint for an AI Bill of Rights

"To advance President Biden's vision, the White House Office of Science and Technology Policy has identified five principles that should guide the design, use, and deployment of automated systems to protect the American public in the age of artificial intelligence."

Why this is important: Automated systems and algorithms are commonplace in today's economy and societal connections. In a recent release, the White House Office of Science and Technology Policy ("OSTP") has released guidance that this administration will seek to apply in developing consumer protections related to automated systems, data, and artificial intelligence. The guidance, which is being called a "Blueprint" points to five principles: 1) protection from unsafe or ineffective systems, 2) equitable use and design for algorithms to avoid discrimination, 3) individual agency related to data use and privacy, including built-in protections from abusive data use, 4) disclosure, explanation, and notice of data uses and the implementation of automated systems, and 5) opt-out provisions and protocols, where appropriate, to have a human alternative to an automated process. There is a good amount of overlap in these five principles, but that is also intentional. The OSTP asserts that the overlap will provide for a "set of backstops against potential harms." The full Blueprint (available now from whitehouse.gov) is the

result of a year-long initiative from the White House, and consists of a 73-page whitepaper and technical companion that outline and describe how these principles can be implemented across a wide range of industries. The principles do appear to be sufficiently general, such that they can be widely interpreted and applied as each industry is best able. --- Brian H. Richardson

---

Are Password Managers the Missing Link When It Comes to Protecting Organizations from Cyber Attacks?

"Passwords have long been the weakest link when it comes to IT security and a leading source of data breaches."

Why this is important: The business community has expended significant time and effort to improve the security of their infrastructure. Despite these efforts, many organizations remain vulnerable due to poor password management practices. Some employees utilize a simple password so that they can easily recall the information. However, this practice can provide a hacker with the opportunity to breach the system. To address this issue, some companies utilize a Single Sign-On which enables users to use one set of credentials to access multiple applications within their system. This method does not provide a solution for applications that are outside of the system such as encrypted documents. As remote working has become more common, organizations run the risk that employees are using unauthorized products or tools that could decrease the security of their data.

Some organizations turn to password management solutions, but these solutions may be unworkable for highly regulated industries as the data is stored outside the organization on the service provider's cloud. Self-hosted solutions can be stored within the boundaries of the company's IT infrastructure, but they require resources to manage the solution. Although each organization will need to examine their business practices and determine how they can best address password security, one thing is clear—failing to implement password security measures is a risk that is not worth taking. --- Annmarie Kaiser Robey

---

The Ethereum Merge is Done, Opening a New Era for the Second-Biggest Blockchain

"The historic upgrade casts aside the miners who had previously driven the blockchain, with promises of massive environmental benefits."

Why is this important: The world's second largest cryptocurrency recently changed how it does business. Ethereum underwent the Merge. Like other cryptos, Ethereum uses a blockchain to record its transactions. Until recently, cryptocurrency miners competed for the privilege of adding the next block to that blockchain. Those miners used rows and rows of specially built computer hardware to solve complicated equations. The locations where they did this are called crypto mining farms, but as the article correctly points out, it's more accurate to call them factories. Imagine a warehouse filled with racks of computer hardware constantly running. They put out a lot of heat, and they soak up a lot of electricity. This use of electricity has been a sore subject recently as people complain about the economic impact of crypto mining. With its Merge, Ethereum has changed from using these miners and farms/factories to a system that's called Proof-of-Stake. In this system, miners are replaced by "validators" who pledge at least 32 of the Ethereum crypto for the opportunity to be selected to add the next block to the blockchain. The effect is Ethereum now should consume 99 percent less electricity. The article cites one commentator that it's like Finland has suddenly shut off its power grid. Ethereum hasn't seen a price surge as a result of changing to the more eco-friendly Proof-of-Stake, but it's still too early to tell whether it will be rewarded for this change. There are no plans for Bitcoin, the world's largest crypto, to follow in Ethereum's tracks, but we wouldn't be surprised to see other cryptos that are large enough to effectively make this switch try to do so and take advantage of being seen as another eco-friendly alternative to Bitcoin. --- Nicholas P. Mooney II

FDA Bill Passes Without Cybersecurity Requirements for Medical Devices

"The bill's passage will 'reauthorize the FDA user fee agreements for five years to ensure the agency does not need to issue pink slips,' Energy and Commerce Committee Chairman Rep. Frank Pallone Jr., D-N.J.,

said in a statement."

Why this is important: In previous issues of *Decoded*, we have discussed the lack of cybersecurity in relation to medical devices. We have also discussed Congress' introduction of the PATCH Act that, if passed, would be a major step forward in securing networkable medical devices. Despite knowing the risk inherent in the lack of sufficient cybersecurity in medical devices, Congress failed to take additional steps to protect medical facilities and patients from the latent defects in networked medical devices when it recently passed an FDA appropriations bill to maintain the FDA's funding. While the funding bill allows the FDA to continue normal operations, the bill failed to include any cybersecurity requirements for medical devices. Originally, the bill included significant cybersecurity requirements drawn directly from the PATCH Act, including the requirement that medical device manufacturers submit premarket submissions that would ensure that a networked medical device met cybersecurity requirements. However, Senate Republicans blocked the inclusion of these cybersecurity requirements in the appropriations bill. Sens. Patty Murray, D-Wash., and Richard Burr, R-N.C. reaffirmed Congress' commitment to cybersecurity for medical devices ahead of the December government funding deadline. In light of government's failure to address the medical device cybersecurity in a timely manner, many are calling on the medical device industry to institute these necessary requirements on its own. --- Alexander L. Turner

---

Pennsylvania Legislators Discuss Consumer Data Privacy

"Providing for consumer data privacy, for rights of consumers and duties of businesses relating to the collection of personal information and for duties of the Attorney General."

Why this is important: Representative Robert Mecuri (R-Allegheny County) and a number of his colleagues have co-sponsored House Bill 2202 Bill.

The legislation would require larger companies and personal information aggregators to provide information on the data that is gathered, tracked and sold. It would also allow consumers to opt-out of the processing of their personal information for the purpose of targeted advertising or the sale of the information.

On September 29, 2022, Representative Mecuri joined his colleagues, Representatives Napolean Nelson (D-Montgomery) and Craig Williams (R-Delaware and Chester County) as well as other privacy experts as speakers at "Pennsylvania: The Next State Consumer Privacy Law?" The event was hosted by the Pittsburgh and Philadelphia chapters of the International Association of Privacy Professionals ("IAPP"). During their presentation, the Representatives discussed the challenge of striking the right balance between providing transparency with respect to data, empowering consumers to make decisions regarding the storage and use of data while providing a compliance structure that is not onerous to businesses. When crafting the legislation, the Representatives examined how other states have approached the issue including California and Virginia. As noted above, HB 2202 contains an opt-out provision. Although some privacy legislation proponents may advocate for an opt-in approach, such a high standard has the potential to reduce the likelihood of the bill's passage.

The legislation was introduced and referred to the House Consumer Affairs Committee on December 13, 2021. The legislation is unlikely to move this session due to the limited number of scheduled session days, but the issue will likely reemerge next session. --- Annmarie Kaiser Robey

---

Big Data Trove Dumped After LA Unified School District Says No to Ransomware Crooks

"Confidential incident reports, personnel records, and more are leaked online."

Why this is important: In our e-newsletter focusing on higher education law - *The Academic Advisor* - we have discussed the recent rise in cyberattacks against school districts and colleges. This discussion was focused on the recent cyberattack on Los Angeles Unified School District ("LAUSD"). This attack affected 540,000 students and 70,000 district employees. The hackers were identified as the Vice Society, a Russian-speaking ransomware group that has previously focused on small and medium size companies as the targets of their attacks. In response to the attack, the LAUSD followed the White House and National Security Council's recommendation that the district not pay the ransom. As a result of the LAUSD publicly refusing to pay the ransom, two weeks ago, the Vice Society published 284,000 files on

its website. The information released included incident reports, social security numbers, attendance records, unredacted passports, and other sensitive information of school employees and contractors. --- Alexander L. Turner