SHARE:

Join Our Email List

View as Webpage

August 3, 2022

Welcome

Welcome to the 15th issue of *Decoded* for the year.

As we wind down the summer and look forward to fall, we want to make sure we are covering the topics you find interesting and could be of help to you and your organization. We would love your feedback. Feel free to email us your thoughts about topics, opinions and any ideas you have for our publication.

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

Data Privacy, Abortion Limits Set to Collide Post-Roe

"Even before the June 24 ruling in Dobbs v. Jackson Women's Health Organization, privacy advocates, concerned that data on women seeking abortions could be used to target them, sounded alarms that women should be vigilant in the types of data and content they share with fertility and health apps and through social media."

Why this is important: Data privacy concerns will collide with states' abortion restrictions in a troubling landscape of uncertainty following the Supreme Court's decision to overturn the federal right to abortion. Only a handful of states have passed data privacy laws -- California, Colorado, Connecticut, Utah and Virginia -- and it's unclear how those laws would affect people seeking abortions across state lines. How and whether local law enforcement agencies and prosecutors would use data to identify people seeking or providing abortion services is unsettled, however the amount of data available is concerning.

Particularly in states that have enacted bounty-style laws, rewarding people who bring successful lawsuits against anyone aiding abortion, there is incentive to dig through digital footprints. Peoples' internet search histories, text messages, emails, location tracking, online payments, and user-generated health information -- such as from fitness or menstrual cycle apps -- are just some of the data points available that could be weaponized against those seeking or providing abortion care. Even a federal data privacy law may not be able to protect against the Dobbs-related risks. Rep. Sara Jacobs, D-Calif., and Sen. Mazie K. Hirono, D-Hawaii, have drafted legislation that would specify that no entity may "collect, retain, use, or disclose personal reproductive or sexual health information" without express permission from an individual or to provide services to the individual. The problem with any data privacy law is that law enforcement can seek a subpoena or court order to force entities to submit certain data -- the same way health providers and plans must adhere to a court order or subpoena, even when HIPAA otherwise prohibits the disclosure of personal health information. --- Alison M. Sacriponte

Breach Rule Would Give Credit Unions Longer Reporting Window than Banks

"The 72-hour time frame falls in line with the Critical Infrastructure Act that President Joe Biden signed in March, but is twice as long as the reporting window banks have had to comply with since May."

Why this is important: The National Credit Union Administration ("NCUA") recently issued a proposed rule regarding a change to the reporting period for credit unions to report cybersecurity incidents. The proposed rule would require credit unions to report cybersecurity incidents to the NCUA within three days of reasonably believing a reportable cyber incident has occurred. This proposed rule change is in conformance with the Critical Infrastructure Act that was signed into law in March 2022, which requires companies to notify the Cybersecurity and Infrastructure Security Agency within 72 hours of learning of a cyberattack. This proposed rule change is less strict than the rule instituted by the Federal Deposit Insurance Corp. ("FDIC") for covered banks. Banks regulated by the FDIC are required to report cybersecurity incidents within 36 hours of discovery. The proposed NCUA rule is likely more lenient because smaller institutions, which most credit unions are, may have difficulty complying with a 36-hour reporting period. --- Alexander L. Turner

Medical Device Cybersecurity: 22 Million US Health Records Breached Thus Far in 2022

"GlobalData forecasts that spending on cybersecurity in the medical device sector will grow from $869 million to $1.2 billion between 2020 and 2025, at a Compound Annual Growth Rate (CAGR) of 7.3%—only accounting for about 11.3% of health cybersecurity spending and 0.6% of the forecast global security spending of $198 billion for 2025."

Why this is important: The title says most of it… 4.6 percent increase in cyber-breaches in the medical device sector. This also provides a summary of some targets for this activity that you may not have considered, such as using your health information to target you with false schemes. --- Hugh B. Wellons

How Technology Amplifies Recognition, Helps Stem Turnover

"Two new studies show how the shrewd use of technology can help deliver more meaningful and frequent recognition to employees in ways that help stem resignations, keep remote workers connected to their colleagues and boost performance."

Why this is important: Sometimes, the best way to know you are doing right by your employees, is to simply ask them. When that seems like a daunting task, technology can help bridge the human nature gap. In studies conducted by Gallup, Workhuman and the Achievers Workforce Institute, key indicators of the benefits of technology in improving employee recognition and retention were revealed. Results indicate that as many as two-thirds of employees indicated that "meaningful recognition" would reduce their desire to job hunt or respond to inquiries from headhunters. The need for improvement is clear when you contrast that figure with the one-quarter of employees currently reporting a sense of meaningful connection with their collaborative co-worker teams. Technological interventions can help to 1) make recognition more frequent and meaningful to individual employees, 2) elongate the duration of a

recognition moment, and 3) flag and help reduce recognition bias among managers. As an example, where managers are able to implement social media platforms to post recognition, others in the company are then able to interact with the recognition "moment" by sharing, "liking" or otherwise re-posting. Each of these create an instance where the employee being recognized is able to be reminded of the recognition. The research indicates that the reminder of recognition activates the same areas of the brain as the initial recognition moment. Companies should absolutely be implementing technology to track and monitor their recognition practices. These data can be critical in ensuring that fair and equitable practices are implemented for recognizing employee accomplishments (and in making sure nobody is feeling left behind on the team). Alternatively, in the unfortunate event of a discrimination suit, the data could also help demonstrate objective evidence of fair practices. Perhaps most importantly, however, is that as many as 73 percent of employees with quality recognition practices are more likely to see a "path to grow" within their organization. --- Brian H. Richardson

Data Breach Exposes Personal Information of Concealed Carry Permit Holders

"California residents with concealed carry weapon permits had their personal information exposed in a data breach during the state Department of Justice's unveiling of its '2022 Firearms Dashboard Portal.'"

Why this is important: Data breaches do not just affect businesses and individuals. Government entities are also targets of cybercriminals. Recently, the personal information of 242,727 California Conceal Carry Weapon ("CCW") permit applicants between 2011 and 2021 were compromised when the California Department of Justice ("CADOJ") suffered a breach of its 2022 Firearms Dashboard Portal. This breach permitted access to the backend of the CADOJ's website, and exposed CCW permit applicants' personal information, including name, address, age, license type, and Criminal Identification Index number. It is unknown how long ago this breach occurred, or how long CCW permit applicants' personal information was exposed, but the compromised portal was only up for 24 hours before the breach was discovered. This breach did not just expose the personal information of CCW permit holders, but also the personal information of individuals who applied for a CCW permit and were denied. The California Sheriff's Association says that this leaked information has been copied and some of it was posted online before the breach was detected. There is also a question of whether the information was accessed by an outside party, or whether the information was posted on the internet by a state employee. In response, the CADOJ intends to contact everyone affected by the breach to work with them to minimize any potential harm related to the breach, including providing them with free credit monitoring. The CADOJ also took down the 2022 Firearms Dashboard Portal to prevent future breaches until it can determine how the system was breached. However, many gun rights organizations say that this is too little too late. They also question the timing of the breach in light of the Supreme Court's recent ruling that effectively nullified California's requirement that CCW permit applicants provide a strong basis for needing a CCW permit. Due to California's strong opposition to the Supreme Court's ruling, gun rights organizations are requesting that an independent investigation be conducted by an entity not affiliated with the California government. Gun rights organizations are also concerned that this breach exposes to criminals who do and who do not have the legal right to conceal carry a gun in California, thereby allowing those whose permit applications were previously denied under the stricter requirement, or who never applied for a permit, to now be exposed to potential harm and criminal activity. Additionally, four women have brought a class action lawsuit against the California Attorney General claiming that he violated their Second Amendment right to keep and bear arms; their Fourth Amendment right to privacy; their right to privacy under the California constitution; and for a violation of California's Information Practices Act of 1977, which limits government use of personal data. The four class representatives are seeking to discover how the breach occurred. They are also seeking compensatory damages and a declaratory judgment that the state collecting personal information in relation to CCW permit applications violates both federal and state law. The National Association for Gun Rights also filed a class action lawsuit against the California Attorney General related to this breach. --- Alexander L. Turner

FDA Patient Advisers Grapple with Consent, Oversight of Virtual-Reality Devices in Healthcare

"An advisory committee provided recommendations to the FDA on patient consent for surgeries that use augmented reality tools and how virtual reality devices used in healthcare should be regulated."

Why this is important: Interesting article about the use of digital tools to improve informed consent. As medical treatment has become more complicated, it has become almost impossible to demonstrate

real informed consent. The technology that is saving lives, even while being difficult to explain, also can help to explain or demonstrate how the technology works and what the risks are. --- Hugh B. Wellons

Tenet Healthcare, Baptist Health Face Healthcare Data Breach Lawsuit

"An investigation revealed that an unauthorized party potentially infected the hospital network with malicious code and was able to remove some data from the network."

Why this is important: In a putative class action lawsuit stemming from a healthcare data breach discovered in April 2022, a Texas-based hospital network is headed to court. The case arises from a data breach caused by malicious code implanted in the hospital's network that mined data affecting approximately 1.2 million patients between March 31 and April 24, 2022. For now, the exact method of unauthorized access remains undisclosed, and is described by the hospital system as affecting only "certain systems." Certifying a class for the lawsuit will likely be an uphill battle, however, in light of the 2021 ruling by the Supreme Court on Article III standing for plaintiffs in data breach incidents. In *TransUnion LLC v. Ramirez*, the high court held that Article III standing was limited in certain instances to plaintiffs that have been "concretely harmed." This may come into play in the Tenet Healthcare case as the defendants will undoubtedly seek to challenge standing for the putative class action. As more details emerge regarding the nature and specifics of the method of unauthorized access, and safeguards put in place to remedy the breach once discovered, healthcare providers will be better informed and prepared to prevent similar breaches in their own systems. --- Brian H. Richardson

Average Healthcare Data Breach Costs Surpass $10M, IBM Finds, Patients Demand Health Data Privacy, Accountability, Transparency and NIST Updates Healthcare Cybersecurity, HIPAA Security Rule Guidance

"The figure signified a 9.4 percent increase from the 2021 report and a 41.6 percent increase from 2020."

"Three-quarters of surveyed patients expressed health data privacy concerns, and nine out of ten patients said they wanted to see companies held accountable for health data use."

"The revision is more actionable so that health care organizations can improve their cybersecurity posture and comply with the Security Rule."

Why this is important: Three articles on general data privacy issues in medical care. Medical data breach frequency is exploding, and people are noticing the problem. Partially as a result, NIST ("National Institute of Standards and Technology") is updating its standards and revising HIPAA guidance. --- Hugh B. Wellons

Ceridian Fingerprint Scan $3.5M Class Action Lawsuit Settlement

"The Ceridian class action lawsuit notes that there are significant risks associated with biometric clocks in the workplace."

Why this is important: Ceridian HMC Inc. has agreed to pay nearly $3.5 million to settle a class action lawsuit alleging that the collection of their employees' fingerprint data violated the Illinois Biometric Information Privacy Act ("BIPA"). The lawsuit alleges that Ceridian collected biometric data when their employees used the company's finger-scan time clocks in Illinois without providing proper notice or obtaining the employees' consent. BIPA is an Illinois law that prohibits private companies from capturing, storing, obtaining and/or otherwise using an individual's biometric data for any purpose without first providing notice and obtaining the individual's written consent. The lawsuit notes that there are significant risks with biometric data such as fingerprints because it cannot be changed if the data

becomes compromised. As companies seek to utilize technological advancements in the workplace, it is important that they proceed cautiously and consult with counsel to ensure they are not running afoul of any laws that place requirements on the organization. --- Annmarie Kaiser Robey