View as Webpage

October 27, 2022

Welcome

Welcome to the 21st issue of *Decoded* for the year.

We are pleased to sponsor the 16th Annual ABA Labor and Employment Law Conference. This signature conference will be held on November 9–12, 2022 in Washington, DC. This year's conference features prominent speakers and exciting and balanced panels; a full year's worth of CLE credit for most jurisdictions; a curriculum covering all aspects of labor and employment law practice; a multi-level program that will be of value regardless of your degree of experience; and opportunities for you to meet with colleagues representing all perspectives in the labor and employment field. You can learn more and register 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

---

EU and U.S. Agree to New Data-Sharing Pact, Offering Some Respite for Big Tech

"For over a year, officials on either side of the Atlantic have been hashing out a deal to replace the so-

called Privacy Shield."

Why this is important: The U.S. and the EU have different approaches to data privacy. The EU, with the General Data Protection Regulation ("GDPR"), has a comprehensive approach to data security that is derived from a central authority. The GDPR provides EU citizens with certain rights, including the right to (1) be informed on how their data will be used, (2) access the data that is collected, (3) rectify incorrect data, (4) have their data erased, (5) restrict how their data is processed, (6) data portability, (7) object to the sale of their data, and (8) not have their data used for automatic decision making. Each EU member state also designates a Data Protection Authority to oversee compliance with the GDPR. EU member nations are allowed to freely share personal data with businesses in countries that have a similar comprehensive system in place to provide data privacy. The GDPR applies to any business located in the EU even if the data it collects is from outside the EU, and to any business outside the EU that collects data from citizens of EU member nations.

The U.S., by contrast, does not have a universal federal data privacy law, but instead follows the sectoral approach to data privacy wherein it has individual laws dictating how data privacy is to be applied on an industry basis. This includes data privacy laws like the Fair Credit Reporting Act in the financial industry, and the Health Insurance Portability and Accountability Act in the healthcare industry, to name a few. Because of structural differences in how the U.S. and the EU approach data privacy and cyber security, businesses in EU member nations are not automatically allowed to share personal data with businesses in the U.S. In order to permit data to flow between the EU and the U.S., there needs to be a negotiated framework in place to allow for the transfer of data between the EU and the U.S.

Previously, the EU and U.S. had an agreed framework in place called the Privacy Shield. The Privacy Shield allowed data from the EU to be shared with businesses in the U.S. under certain circumstances. However, in July 2020, the Privacy Shield was invalidated by an Austrian court that said the Privacy Shield did not sufficiently protect EU citizens from surveillance by U.S. companies. This was a significant problem for companies like Facebook, Meta, and Instagram because a significant portion of their income comes from the sale of personal data. Without the Privacy Shield in place, they were unable to collect and sell the data of their EU customers, and were considering shuttering their EU operations as a result. However, earlier this year, the U.S. and EU were able to negotiate a new framework, the Trans-Atlantic Data Privacy Framework, that allowed for the renewed flow of data from EU member nations, while protecting EU citizen's data privacy rights. Companies like Facebook, Meta, and Instagram were relieved that they were again able to operate in EU nation states, with the new agreement anticipated to produce $7.1 trillion in economic relationships with the EU. --- Alexander L. Turner

---

Key Ways to Manage the Legal Risks of a Healthcare Data Breach

"Managing the legal risks of a healthcare data breach requires organizations to view risk holistically and collaborate with key stakeholders."

Why this is important: Successful management of legal risk can make an enormous difference in outcomes from a healthcare data breach. Prevention is key, but when breaches do occur, managing (and mitigating) legal risk can be helped by remembering certain best practices. This article provides great insight into ways that can be accomplished. First, be aware that a healthcare organization's notification obligations in the event of a data breach will vary from state to state. There is not a nationwide protocol for notification requirements. Organizations should be aware and stay up-to-date on the applicable regulations for the jurisdictions in which they operate. Second, remember that proper documentation is critical to managing risk. Documentation takes place well before a data breach. Organizations should be purposeful in documenting their internal review, assessment, testing, and remediation protocols and practices as well. Legal risk in a claim of negligence, for example, will often turn on what practices were

in place, and how the organization implemented and updated those practices to stay up-to-date with new risks. Third, maintaining and updating a cyber incident response protocol will allow for swift mitigation in the event of a data breach. Finally, collaboration across intra-organization divisions is also critical. Appropriately de-silo your organization to maintain a continuity of security best practices, and to gain insight from departments. --- Brian H. Richardson

---

Overview of State Data Privacy Legislation and Potential Pitfalls to a Unified Federal Approach

"The U.S. government's approach in the privacy arena further contrasts with the European Union's omnibus approach, where the latter has developed the comprehensive General Data Protection Regulation to provide individual control and rights over personal data."

Why this is important: We have discussed in previous editions of *Decoded* about pending legislation before Congress that would create a universal federal data privacy law in the U.S. Currently, five states have passed comprehensive data privacy laws. The state laws give citizens of California, Colorado, Connecticut, Utah, and Virginia the basic rights to (1) access personal information, (2) to correct inaccurate information, (3) to delete information, (4) to limit the use of data for profiling or targeted advertising, (4) data portability, and (5) opt out of the sale of personal information. Other states, like Illinois, have limited data privacy laws that protect against improper collection of biometric data. With the proposed federal data privacy law, the question becomes how it will be implemented in light of states having their own data privacy laws. Will it preempt state data privacy laws, and if so, to what extent? Businesses want a federal data privacy law in order to avoid having to comply with and defend against a patchwork of 50 different data privacy laws across the country. Data privacy advocates, and states like California, fear that a weak federal data privacy law will preempt stronger individual state data privacy laws. Additionally, California is opposed to the House bill because it does not provide for a private right of action, which is guaranteed in the California Consumer Privacy Act. Consequently, the House bill will likely stall because of the issues of preemption and the ability to bring a private cause of action. --- Alexander L. Turner

---

Why the Healthcare Industry Needs to Adapt Physical Layer Visibility

"And, with the astonishing, overwhelming amount of new IoMTs and IoTs being introduced to healthcare facilities, having an accurate asset inventory, maintained in real-time, is paramount for establishing top-notch cybersecurity."

Why this is important: "We are fighting a war with no front lines." Healthcare delivery organizations can learn a lot from these words, delivered to a joint session of Congress by General Westmoreland while he was serving as commander of all U.S. military forces in Vietnam. The concept of physical layer visibility refers to understanding the full infrastructure of an organization's data and IoT footprint – and being able to readily access it. This goes from a holistic overview at the first layer, down to the specific devices and components at deeper layers. This article provides valuable insight into four key elements (and benefits) of implementing Layer 1 visibility for healthcare delivery organizations. 1) Complete asset visibility, 2) Hardware access control, 3) Continuous device operability, and 4) Regulation (and compliance). Healthcare organizations should really think of physical layer visibility as a mechanism for identifying and managing vulnerabilities across the organizational infrastructure. In other words, in providing for cybersecurity of data and protecting patients, adopting and adapting physical layer visibility protocols effectively reestablishes the "front lines" again. --- Brian H. Richardson

Bloomingdale's Class Action Alleges Company Wiretaps Customers' Electronic Communications

"Bloomingdales.com LLC secretly intercepts customers' electronic communications when they visit the retailer's website in violation of Missouri's wiretapping law, according to a recent class action lawsuit."

Why this is important: A class action lawsuit has been filed against Bloomingdale's for an alleged violation of the Missouri Wiretap Act and the privacy rights of consumers who visit the store's website. It is alleged that through the use of a third-party vendor, Javascript code is embedded in the website which allows for the recording of the consumer's keystrokes so that the consumer's experience can be replayed for Bloomingdales. The litigation further alleges that sensitive personal information such as medical conditions and credit card information may be captured during the recording. Bloomingdales is not the only business facing such litigation as Casper Sleep recently faced an invasion of privacy class action lawsuit challenging the use of keystroke monitoring software on its website.

As businesses seek to obtain information from consumers regarding their online experiences to develop marketing strategies, they should be mindful of the types of information that is being gathered and analyzed and ensure compliance with applicable laws and regulations. Furthermore, it would be wise for businesses to seek ways to narrow their focus when gathering information so that they are not inadvertently capturing sensitive personal data. --- Annmarie Kaiser Robey

---

Gen Z, Millennial Workers are Bigger Cybersecurity Risks than Older Employees

"Younger workers surveyed are less likely to follow established business cybersecurity protocols than their Gen X and baby boomer counterparts, a new survey finds."

Why this is important: Stereotypes can be risky business for cybersecurity. Gen Z and Millennial workers are stereotypically thought of as being more tech-savvy than their more senior colleagues. However, familiarity with technology is not the same thing as cybersecurity. Market watchers are finding that the younger generation of workers may actually pose more of a cybersecurity behavior risk for their employers. Ernst & Young's EY US Consulting Group has released the inaugural report of what is anticipated to be an periodic survey into cybersecurity practices among adult workers in the United States. The 2022 EY Human Risk in Cybersecurity Survey polled 1,000 "tech-enabled professionals" – defined as adult individuals currently employed in the United States that had been issued a work-owned laptop/computer device. The results give insight into the self-reported practices related to human risk in cybersecurity protocols across a range of industries, ages, races, genders, and regions. Three specific metrics stood out as indicators where younger employees self-reported more risky behavior: 1) disregarding or delaying mandatory IT updates, 2) reusing passwords for work and personal accounts, and 3) routinely accepting browser cookies. In addition, nearly half of all Gen Z and Millennial workers surveyed admitted to being more cautious with their personal devices than with their work devices. These findings should absolutely be reviewed by enterprise security teams, IT professionals, and company policy makers in developing their training protocols. Human behavior (and social engineering) remain the leading cause of data breaches and cybersecurity incidents nationwide. Training protocols should be specifically tailored to meet the needs of a company, including developing incentives for employee compliance with existing policies and procedures. One effective option may be as simple as having employees re-affirm their agreement and acknowledgement of cyber policy. For example, if your company policy requires that passwords for work systems be unique and not reused for personal

accounts, then your IT team could build in an acknowledgement and reminder of this policy whenever a periodic password reset takes place. This would give non-compliant employees an opportunity (and nudge) to comply. --- Brian H. Richardson

---

Share This Email | Share This Email | Share This Email