SHARE:

Join Our Email List

View as Webpage

September 29, 2022

Welcome

Welcome to the 19th issue of *Decoded* for the year.

Do you have topic ideas for *Decoded*? Do you have specific questions you feel would be of interest to other readers? Would you like to see a webinar addressing a certain area? Let us know! We have a large group of attorneys with a wide range of disciplines that could address your specific topic.

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

Seven North Carolina Colleges Secretly Tracked Social Media Posts of Students, Protesters

"A new report shows seven North Carolina universities monitored social media platforms to keep an eye on things like protests or crimes."

Why this is important: Developers of social media surveillance software sell their products to colleges and universities as a tool that scans social media to identify students who may be a danger to themselves or others. But a number of schools have been using these tools for a different purpose -- surveillance against student protests. It recently was reported that seven North Carolina colleges, both public and private, have been secretly tracking students' social media posts in relation to protests by students regarding the abortion debate and other controversial issues. This tracking is seen as the latest in campus security protocols that started with blue light phones in the 1980s, moving onto CCTV cameras 1990s, and then included building access controls in the early 2000s. Designers of these social media trackers skirt around privacy concerns by saying that they are not investigating or actively surveilling students. They say that they are only monitoring public social media to identify safety and security related information. Despite this assertion, at least one company, Social Sentinel, has promoted its product to “mitigate” and “forestall” student protests. These third party monitoring companies are also expanding their services to include monitoring student emails sent on school accounts. This student monitoring does raise a number of concerns. One issue with this technology is that it may stifle students’ freedom of expression because people who know they are being surveilled are more likely to self-censor. Additionally, these companies are using AI that is untested, and has a risk of being abused. Finally, the public schools that use this service run the risk of violating their students’ Constitutional rights to free speech and protections against illegal search and seizure. While safety on campus is paramount, schools need to consider how these tools may impact campus culture and students’ rights before utilizing this technology. --- Alexander L. Turner

Instacart Announces New Connected Stores Technology

"Connected Stores aims to create a unified, personalized experience for customers by enabling them to move seamlessly between a retailer’s app or website and its physical, in-store experience."

Why this is important: Some consumers enjoy having their groceries delivered, while others prefer the in-person experience. Instacart is implementing technological changes to improve the customer experience. The new technologies include Caper Cart (smart carts allow self-checkout without scanning items), scan and pay (scan items and pay on your mobile phone), Lists (syncs your shopping lists from the Instacart App or a grocer’s app and locates items in the store), Carrot Tags (electronic shelf labels help customers locate items), FoodStorm Department Orders (helps retailers efficiently manage specialty food orders), and Out of Stock Insights (provides alerts to retailers when items are running low).

These new technologies will be added to existing Instacart capabilities to create Connected Stores. Connected Stores seek to create a personalized consumer experience that provides the user with a seamless experience whether they are using the app, website or walking around the store. The first Connected Store is being built in Irvine, California through an Instacart and Good Food Holdings partnership.

Food delivery apps were widely used during the pandemic and many individuals continue to use them. Instacart’s technological additions will allow consumers the ability to select the options that best meet their needs. To remain competitive, businesses will need to ensure that they are in tune with consumer needs and provide the tools required for a positive experience. --- Annmarie Kaiser Robey

Green Tea Molecule Can Break Up Protein Tangles in the Brain that Cause Alzheimer’s

"The green tea molecule, EGCG, is known to break up tau fibers -; long, multilayered filaments that form tangles that attack neurons, causing them to die."

Why this is important: UCLA scientists have found that EGCG, a molecule in green tea, can break up protein tangles in the brain that are believed to cause Alzheimer’s and similar diseases. Tau fibers are “long, multilayered filaments that form tangles that attack neurons, causing them to die.” The death of the neurons is what causes Alzheimer’s and other similar diseases. Scientists believe that if they can remove or destroy the tangles then they can slow the progression of the diseases. The discovery that EGCG destroys the protein tangles has led to further studies being conducted with other molecules. Molecules known as CNS-11 and CNS-17 have been shown to stop these tau fibers from spreading to other cells. These molecules, and others, were tested using computer simulations to determine if the molecules would attach to the tau fibers and cause them to break down before any wet-lab experiments were conducted. Further testing was done by extracting the tangles from the brains of people who have died from Alzheimer’s and incubating them with EGCG for different time periods. After three hours, about half the tangles were gone and the others were partially degraded. Within 24 hours, all of the fibers were gone. The advancements in technology and the discovery of these molecules can lead to further treatments to stop the progression of diseases such as Alzheimer’s and Parkinson’s. --- Grace K. Dague

DOE Invests $12M in Cybersecurity Research for Energy Grid

"Meanwhile, the concern over energy grid attacks has increased with the Russian attack on Ukraine."

Why this is important: The Secretary of the Department of Energy and a former FERC chairman agree that our country’s enemies could shut down the U.S. power grid. To fight against that prospect, the DOE recently announced $12 million in funding to create six research programs aimed at improving power substation design, cyber threat detection, and cyber defense systems. The article also discusses the recent Cost of a Data Breach Report (the average cost of a data breach worldwide in 2021 was $4.65

million). The energy industry was ranked fifth in costs of a data breach, and most attacks in the energy industry were social engineering attacks. There currently is no way to prevent a cyberattack from occurring, but companies can take the following steps to guard against social engineering attacks:

- Conduct regular security awareness training.
- Implement a social media policy that addresses privacy and posting.
- Enable multi-factor authentication.
- Conduct simulated phishing campaigns.
- Train employees on the increase in smishing attacks (cyberattacks by texts).
- Retain a third party to conduct penetration testing and simulated social engineering attempts.
- Determine your company's critical assets and implement continuous monitoring of those assets.
- Implement cybersecurity policies and procedures and/or review current policies and procedures for any needed updates. --- Nicholas P. Mooney II

A Cautionary Tale: Sharing Your Riskiest Insider Threats is a Culture Killer

"When we cast a large shadow on what we consider to be an insider threat, the threat itself has just that; a bigger shadow."

Why this is important: Cybersecurity threats from inside your own organization have been increasing in frequency and cost. In response, executives are taking notice and are trying to curb this rising trend with innovative new solutions. Organizations need to be able to detect and mitigate threats posed by insiders faster. In order to accomplish this, "key objectives such as proper data access monitoring and control, strict DLP policy, IDS/IPS to allow for event prevention, SIEM or log analysis, strict IAM (Identity and Access Management), and a robust vulnerability management program must be implemented." However, while these solutions are effective, leadership has to be careful that they do not allow the fear of an insider threat damage company culture. This fear pits leadership against their own employees, creating distrust and resentment in the ranks because the threat may be defined so broadly that everything becomes an insider threat. The proper way to address insider threats is not to see the user as having become more negligent, but instead analyze the chain of events that caused the data breach. Therefore, vigilance against insider threats has to be balanced with not alienating your staff and destroying your organization's culture. --- Alexander L. Turner

US Government Rejects Ransom Payment Ban to Spur Disclosure

"Federal authorities strongly discourage organizations from paying ransoms, but Anne Neuberger of the National Security Council explains why it decided against a ban."

Why this is important: The U.S. government rightly put a practical result over ideological stance on this issue. The National Security Council was considering whether to implement a ban that would prohibit individuals and companies who suffer a ransomware event from paying the ransom. It ultimately decided against a ban. Whether to pay a ransom and whether to prohibit individuals and companies from paying is a tough issue. But, it's hard to get around the thought that a ban essentially is punishing the crime victim for the crime. The NSC instead is encouraging individuals and companies not to pay a ransom, improve their cybersecurity defenses, backup data daily, implement multi-factor authentication, and immediately contact government authorities for assistance when a ransomware event does happen. The advice here is sound; making systems secure may require financial investments, but so does paying a ransom. --- Nicholas P. Mooney II

CFOs Should No Longer View Cybersecurity as Insurance

"Investing in emerging technologies to leverage data adds dynamic cybersecurity challenges."

Why this is important: Data and cybersecurity are the responsibility of all executives, including CFOs. In a recent survey, 79 percent of responding CFOs have encountered a data breach in the past 18 months that has resulted in a compromise of the company's data or a financial loss. Because these breaches impact an organization's financial well-being, it is imperative that CFOs be included in the organization's cybersecurity implementation. As with any type of security, the cost of the efficient use of data rises equally with the cost to secure it. As the organization decides to use data in a new way, the vulnerability of that data increases. To protect the organization and its data, CFOs need to equally allocate funds to data innovation and cybersecurity. In order to secure data, the CFO has to do an inventory of all of the data the organization holds. This includes putting a value on the different types of data because an organization can lower its risk by getting rid of unnecessary or low value data. Then funds can be properly allocated to secure the high value data that the company maintains. This should be followed up with periodic audits, and data monitoring in order to ensure sufficient protections are put in place while allocating adequate funds to provide protection for the organization's most valuable data. --- Alexander L. Turner

High-Tech Face Mask can Detect Covid in 10 Minutes and Warn the Wearer Via an App

"Just 10 minutes after coming into contact with the air-borne infections, wearers will be warned so they can take evasive action to stop the spread of the infection."

Why this is important: Scientists have developed a face mask that can detect the bird flu, swine flu, and COVID, and, within 10 minutes of coming into contact with the viruses, the wearer will receive an alert through an app on their phone warning them that they have been exposed. These masks have been tested by researchers in China by placing them in an enclosed chamber and spraying them with liquid containing the proteins found in the viruses. The results of the research showed that the sensors in the masks responded to between 70 and 560 times less liquid than the amount in one sneeze. These masks, while not available yet, could work to help the lower the spread of these diseases by alerting people that they have been exposed without having to go through testing for the diseases, such as nasal swabs. --- Grace K. Dague

Industrial Control Systems Face More Cyber Risks than IT, Expert Testifies

"Most ICS technology was designed more than 20 years ago and built without cyber resilience, Idaho National Laboratory's Vergle Gipson said."

Why this is important: Because of their age, operational technology systems are seen as more vulnerable to cyberattacks than information technology systems. They were designed before there was a clear understanding of how to build cyber defenses into those systems and before the rise in recent years of the sophistication of cyberattacks. As a result, many of these systems are vulnerable to attack. The article advocates that, as the U.S. is upgrading and replacing infrastructure, it is the perfect time to introduce cyber security into the design. This is the right advice. Implementing security-by-design into any system is far better than trying to create a Frankenstein patchwork of security components. --- Nicholas P. Mooney II

Construction has a $3 Trillion Waste Problem. Can Drones — and Digital Twin Tech — Solve It?

"Rather, they'll fly the entire construction site continuously and autonomously, mapping 3D space and uploading the visual data to BIM platforms — building information modeling systems — to ensure that everything stays on track."

Why this is important: Cutting down waste on construction job sites preserves resources and is more cost effective. Much of the waste associated with large construction projects is the result of bad information. In Japan, Exyn Technologies is trying a pilot project to cut down on construction waste by providing real-time information regarding the status of the project. Typically on large construction projects, the general contractor, engineers, and architects walk through the project to personally map the progress of the project, and schedule when certain trades start their portion of the project. This is very time consuming and not possible to perform in real-time. Exyn has a possible solution to this. Exyn plans to use aerial drones to continuously 3D map a construction site, and then upload that visual data to Building Information Modeling ("BIM") platforms. However, Exyn has considerable challenges to overcome. Construction sites are an ever-changing environment where the drones need to be able to navigate changing and moving obstacles. These drones will likely need to use various sensors and possibly AI to be able to operate as intended. But if Exyn is able to overcome these challenges, then it will be able to save construction companies, engineers, and architects a tremendous amount of hours managing a project.

While this would be an incredible advancement in the construction industry, there are legal considerations that need to be contemplated before this technology can be deployed in the U.S. First, since these are aerial drones, the operation of these drones must first comply with Federal Aviation Administration ("FAA") regulations that govern small unmanned aircraft. Contractors or owners will need to obtain waivers from the FAA before they are able to operate these drones on their job site, and this process can take months. The drones must first be registered with the FAA and be operated by an individual who has been issued a remote pilot certificate by the FAA. These regulations are continuously evolving as technology continues to advance, so it is unclear at this time if the FAA would allow autonomous drones to operate on an active worksite. The altitude of the drones is also limited to 40 feet, unless it is within 400 feet of a structure, so the drones should be able to be operated close to structures that are being built higher than 40 feet. The biggest complication for the use of drones on a worksite is that the FAA will not allow the drones to be flown over people who are working on the jobsite unless the FAA grants a waiver. Additionally, the FAA will only permit drone flights during the day. The drone also has to stay in the sight of its controller, and cannot enter restricted airspace.

In addition to FAA regulations, there are additional legal considerations that need to be taken into account before drones can be flown over an active job site. State and local laws need to also be considered before deciding to fly drones over the project. For example, in California, anti-paparazzi laws create invasion of privacy liability if the drone is knowingly flown without permission into another property's airspace in order to capture images. Similar privacy concerns are present related to construction workers and visitors to the jobsite. This is because the movement of the drones to capture images may support an argument that they are infringing on the workers' and visitors' reasonable expectation of privacy. Therefore, before a drone is used to surveil a jobsite, notice must be given to, and consent received from, the workers and visitors on site. Finally, the use of drones has its risks, including possible injury to those working or visiting the project. If there is an accident on-site involving a drone, and it causes $500 or more in damage, then an accident report must be filed with the FAA.

Before deploying aerial drones on your next project, the American Bar Association has outlined a few suggestions for inclusion in contracts, policies, and procedures related to drone operations on jobsites:

- Review national, state and local laws and regulations applicable to the job site;
- Create/update site visit release forms, employee materials and job site signage to facilitate notice and consent regarding drone flights and imagery;
- Develop procedures for drone accident reporting and response;
- Incorporate provisions for obtaining and preserving drone imagery, data and other records into litigation hold memos, document collection checklists, and discovery requests; and
- Develop contract provisions or a drone rider allocating costs of using drone technology and responsibility for complying with applicable laws. Such provisions might address:
  - Who may use drones at the site and under what conditions?
  - Qualifications and vetting for pilots and drone companies and who contracts with them and coordinates their services.
  - Who oversees drone planning and operations, provides notice to and collects releases from neighbors, workers and site visitors as needed?
  - Allocation of costs for drone operations, software and data storage.
  - Indemnities and limitations of liability.
  - Insurance requirements.
  - Safety and communication plans and training requirements.
  - Cybersecurity measures.
  - Intellectual Property rights.
  - Who will process, distribute and store the data, who may access it, by what means, and for what purposes may it be used?
  - Who will keep flight logs and records, for how long, and who can access them?
  - Post-project retention and archiving requirements for imagery, data and records.

While drones can be a tremendous time and cost saver, their implementation does add complications to the management of a construction project. Spilman's construction practice group is available to assist you if you want to utilize drones, or if the general contractor or owner wants to utilize drones, on your next project. --- Alexander L. Turner

f Share This Email | Share This Email | in Share This Email

This is an attorney advertisement. Your receipt and/or use of this material does not constitute or create an attorney-client relationship between you and Spilman Thomas & Battle, PLLC or any attorney associated with the firm. This e-mail publication is distributed with the understanding that the author, publisher and distributor are not rendering legal or other professional advice on specific facts or matters and, accordingly, assume no liability whatsoever in connection with its use.

Responsible Attorney: Michael J. Basile, 800-967-8251