View as Webpage

Issue 3, 2020

The Editors' Note

Welcome to the third issue of Decoded, Spilman's e-newsletter focusing on technology law, including data security, privacy standards, financing technologies, and digital-based means of conducting business.

As with any of our publications, we appreciate your feedback. If there is a certain area or industry you would like to hear more about, please let us know. Likewise, if you think we should send this e-newsletter to your friend(s) or colleague(s), or if you would like to be removed from this mailing, please email us.

We hope you find this information useful and look forward to your feedback. Thank you for reading.

Spilman Thomas & Battle Technology Practice Group

Three People have been Charged for Twitter's Huge Hack, and a Florida Teen is in Jail

"He's accused of being the 'mastermind' behind the biggest security and privacy breach in Twitter's history, one that took over the accounts of President Barack Obama, Democratic presidential candidate Joe Biden, Bill Gates, Elon Musk, Kanye West, Apple, and more to perpetrate a huge bitcoin scam on July 15th."

Why this is important: This article is important because it discusses how "the biggest security and privacy breach in Twitter's history" was masterminded by a 17-year-old living in Tampa, Florida. Two others also have been charged, and an unidentified minor in California has admitted to helping sell access to Twitter accounts. According to an affidavit submitted in support of the charges, the mastermind "allegedly convinced a Twitter employee that he worked in the Twitter IT department and tricked that employee into giving him the credentials" to carry out the scam. The mastermind of the hack then was able to use those credentials to access Twitter accounts of public figures like former President Barack Obama. He then posted on their accounts individual tweets that appeared to come from the accountholder and that said if a user sends Bitcoins to accountholder, he or she will send them back double or donate those Bitcoins and others to a charity. After receiving approximately $117,000 in Bitcoins, the 17-year-old moved the coins to another account. In addition to scamming Twitter users out of Bitcoin, the attackers are alleged to have accessed several users' direct messages and obtained large amounts of data from other users. The author discusses how this type of hack could have been much worse. As society spends more time communicating through social media like Twitter, people have become accustomed to accepting the information they see there. The article quotes law enforcement's statements about the potential outcomes of a hack like this: it "could have had a massive, massive amount of money stolen" and, because the accounts of powerful politicians were hacked "could have undermined politics as well as international diplomacy." --- Nicholas P. Mooney II

Pa. House Panel Weighs Bill that Would Authorize Robot

Deliveries of Groceries and Packages

"Proponents of the legislation say the bill will move the state forward in terms of technology. And the devices limit human to human contact in a time of a global pandemic."

Why this is important: Anyone who has watched an Amazon delivery progress, stop-by-stop, toward its final destination knows that delivery technology has made major strides in the past decades. But, there is still significant room for improvement. And perhaps nowhere is this more true than in the area of last-mile delivery, that part of the delivery process in which shipments move from a transportation hub to a final delivery destination. One of the most promising solutions lies with autonomous vehicles, but existing regulatory structures have limited their deployment. Now, Pennsylvania is considering a limited authorization for autonomous delivery vehicles that would restrict their use to sidewalks and roadway shoulders, as well as their speed. For some opponents of the measure, however, even this limited authorization is too much: they argue that it fails to account for pedestrians and the wear-and-tear to sidewalks. At least for now, though, the legislation appears to be on track for passage, having cleared its first hurdle in the Pennsylvania Senate. --- Joseph V. Schaeffer

---

T-Mobile Sued for Allowing $8.7M Cryptocurrency Hack Via SIM Swap

"The plaintiffs alleged that recently, bad actors have been 'using schemes to access customer personal and financial information by causing unauthorized changes in customers' wireless accounts."

Why this is important: T-Mobile was sued in the Eastern District of New York for failure to protect its customers' financial information, which allegedly caused the customers to lose approximately $8.7 million worth of cryptocurrency. A group of hackers utilized a scheme whereby they would convince mobile phone carriers, including T-Mobile, to transfer access to a targeted person's phone number SIM to the hackers' SIM. Hackers specifically targeted accounts that contained large quantities of cryptocurrency. This method is particularly effective because once hackers gain access to the SIM card information, they can control the target's phone, which typically contains sensitive and private information. Many mobile phone owners bypass two-factor, or even one-factor, authentication on their personal devices because the owners are the only users of the phone. When a hacker or other "bad actor" gains access to a user's mobile phone, he or she also gains access to much of the user's private information. In this case, the private information was cryptocurrency locations and wallets. A majority of the global population are users of mobile smartphones, especially the American population. One major point in this case that is important to highlight is the fact that many smartphone users do not protect their mobile smartphone data beyond a simple password or other biometric authentication. These safeguards are effective against outsiders gaining access to the device; however, it does not prevent hackers from gaining access to the information stored on the device through other means. Another key point is that cryptocurrency was the major target. Presumably, the hackers in this case also had access to their targets' bank records and accounts. However, hackers typically steer away from theft of banking information when cryptocurrency is also readily available. With the heavy regulation in the banking industry and the identity theft measures in place to protect the consumer, banking information is protected beyond the user's mobile device. Cryptocurrency on the other hand, is not subject to the same regulation or protection. Therefore, it is a more attractive target to bad actors because the remedies to recover cryptocurrency are not as readily available as other types of financial information. --- P. Corey Bonasso

---

Facebook Adds $100M to Facial Recognition Settlement, Totaling $650M

"Facebook added $100 million to a previous class action settlement to satisfy a skeptical judge, who believed that Facebook was not adequately punished in the original $550 million proposed settlement; the revised settlement addressed these concerns regarding Facebook's alleged unauthorized use of facial recognition technology in violation of the Illinois Biometrics Information Privacy Act."

Why this is important: For data privacy advocates, few laws have been more effective at protecting consumer privacy than Illinois' Biometrics Information Privacy Act ("BIPA"). Although adopted in 2008, BIPA has kept pace with rapid technological developments and provides consumers a remedy for even technical violations of the statute. And as companies that have found themselves on the wrong side of a BIPA claim can attest, resolving those violations can be expensive. Facebook's experience is just the most recent example, and it should serve as a reminder that incorporating a regulatory survey into product development plans is not just an important compliance practice, but a wise fiscal practice, as well. --- Joseph V. Schaeffer

OCC Allows Banks to Hold Cryptocurrency Assets for Safekeeping

"Gould's letter does not carry the weight of a regulation, but it could serve as a road map for banks considering offering cryptocurrency services, which have largely been provided by other types of firms."

Why this is important: The Office of the Comptroller of the Currency recently published an interpretive letter that clarified that "bank custody services" specifically includes a bank "holding the unique cryptographic keys associated with cryptocurrency." As more industries accept the legitimacy of cryptocurrency, the U.S. government seems to be following suit. Demand for cryptocurrency is increasing and highly regulated industries, such as the banking industry, are adapting to meet the growing needs of its customers. The letter specified that banks may offer cryptocurrency services such as actual storage of "tokens" or storage of keys, which are complex passwords that allow access to the currency. However, banks must "effectively manage the risks and comply with applicable law" in order to properly offer digital currency services. The question of "how does one effectively manage the risks and comply with applicable law" as it relates to cryptocurrency is a largely unanswered one. While not an actual regulation, this letter may be a crucial factor in providing some welcome clarity on the issue of cryptocurrency services offered by banking organizations. --- P. Corey Bonasso

---

Geotagged Social Media Posts Didn't Support Personal Jurisdiction–Court of Master Sommeliers v. Pilkey

"However, in personal jurisdiction cases, anything that indicates that the defendant knew it was interacting with a state could be used as evidence of knowledge or intent of the geographic implications."

Why this is important: Despite the above concept that could establish personal jurisdiction, this article analyzes a case where merely geotagging social media posts does not establish personal jurisdiction. In this case, the defendant had passed the "master sommelier" exam. However, the plaintiff later learned that someone had leaked the exam, resulting in almost 2 ½ times the number of individuals passing that exam as earlier ones. The plaintiff canceled the test results. Defendant had passed the exam in question and included on his social media pages that he was a master sommelier, despite the cancellation of the exam results. The plaintiff filed suit for trademark infringement, and, although defendant was located in Chicago, it sued him in California. He challenged personal jurisdiction in California. In response, the plaintiff pointed to several of defendant's social media posts, which included geotagging locations in California as well as a winery located in California, and also argued that it is widely accepted that California makes exceptional wines. The court disagreed with the plaintiff that this sufficiently established personal jurisdiction over the defendant in California. If it had, as detailed in the article and in the words of the court, "Plaintiff's argument would sweep a citizen of any state making a personal social media post about wine under the aegis of California courts simply because much good wine is made in California," . . . and "[u]nder Plaintiff's logic, anyone who has purchased a California wine and tagged a picture in Napa Valley on a personal Instagram account would be subject to personal jurisdiction there." The court also noted that the posts were not advertisements that were part of a marketing campaign aimed at generating revenue aimed at the California wine industry. --- Nicholas P. Mooney II

FCC Issues $2.8 Million Fine Against Drone Manufacturer

"HobbyKing was fined $2,861,128 after '[a]n FCC investigation found that dozens of devices marketed by the company transmitted in unauthorized radio frequency bands.'"

Why this is important: Consumers have made drones a big business in areas ranging from action photography to professional racing circuits. But while drones are being adopted by wider segments of the population, their use is tightly regulated. Many of these regulations are consumer-oriented, governing everything from whether they must be registered to where they can be used (and under what conditions). But, other regulations are manufacturer-oriented and govern their technical capabilities. And as HobbyKing recently discovered, violating those regulations can result in significant financial consequences. For other businesses in this and other emerging industries, HobbyKing's experience should serve as a reminder that a strong regulatory compliance program is not just legally necessary, but also can make long-term financial sense. --- Joseph V. Schaeffer

---

Local Craigslist Ads are Part of Interstate Commerce–US v. Luong

"'By using a website that facilitates interstate commerce (like Craigslist) to advertise a commercial transaction, Luong necessarily affected or potentially affected 'commerce over which the United States has jurisdiction.'"

Why this is important: Aside from being a cautionary tale to anyone using a website to purchase or sell things to strangers, this article is important because it discusses whether placing an ad on a site like Craigslist that involves interstate commerce, even though the sale resulting from the ad does not involve interstate commerce, can be sufficient to support federal criminal charges. In this case, Luong advertised a car for sale in a subsection of Craigslist's East Bay Area (San Francisco) page. The buyer was from the area, and they planned to meet in the same area for the buyer to take a test drive. During the test drive, Luong robbed the buyer at gunpoint. The federal Department of Justice brought criminal charges against Luong. Luong challenged the federal government's ability to charge him since the crime happened in California and both he and the victim resided in California. The court disagreed. It found that Craigslist is structured geographically in that users can't perform a global search across all of its databases but rather must search for items in a particular locale. However, users aren't restricted to searching only in the locale in which they reside, and Craigslist promotes links to other nearby locales, some of which are across state lines. In the end, the court noted that Craigslist facilitates commerce on a national and international level. There is no restriction that prevents an individual from selling to or buying from an individual in another state. In fact, the court found that Luong previously had sold items to individuals living in other states and received inquiries about his car for sale from other states. This article also is important because it notes the frequency that people are charged with robberies facilitated by ads on Craigslist. --- Nicholas P. Mooney II

Today's 'Mega' Data Breaches Now Cost Companies $392 Million to Recover From

"Compromised employee and insider accounts, as highlighted by the recent Twitter hack, are one of the most expensive factors in data breaches today, bringing the average cost of a data breach up to $4.77 million."

Why this is important: IBM's "Cost of a Data Breach Report 2020" provides a sobering analysis for business leaders. The average data breach costs just under $4 million, with that average rising to $4.77 million when compromised employee and insider accounts are involved. And the average cost of "mega" data breaches, those involving more than 50 million user accounts, is now a staggering $392 million. Nearly 40 percent of those breaches involve cloud misconfigurations or stolen or compromised account information, the latter of which can be particularly damaging given the higher likelihood that the breach will result in consumer data exposure. Despite its grim assessment, however, IBM offers some hope for reducing risk, particularly by employing artificial intelligence and automation tools that it claims can cut incident response times by as much as 27 percent. And given the significant operational, reputational, and regulatory consequences, businesses should give these investments serious consideration. --- Joseph V. Schaeffer

---

Repeated Amazon Purchases Sufficient to Impute Notice of Arbitration Clause

"This lawsuit involved weight-loss products, purchased on Amazon, which had been removed from the market at the FDA's request."

Why this is important: This article is important because it discusses a recent unpublished decision of the federal Second Circuit Court of Appeals in which an individual's later purchases were used as a basis for enforcing an arbitration provision in a lawsuit arising from an earlier purchase. That lawsuit involved the plaintiff's purchase of a weight-loss product from Amazon.com. The plaintiff filed suit over the purchase, and Amazon moved to compel the plaintiff's claims to arbitration instead of litigation. The trial court initially ruled in Amazon's favor, but the Second Circuit Court of Appeals reversed that ruling, finding that the terms Amazon used when the plaintiff originally created his account did not contain an arbitration clause. The parties continued litigating, and the issue of arbitration again went to the Second Circuit Court of Appeals. This time, Amazon argued that its account terms now include an arbitration provision and it provided the plaintiff notice of that provision when it previously moved for arbitration in the lawsuit. Amazon then argued the plaintiff had made at least 27 subsequent purchases from it, and

those purchases confirm that the plaintiff agreed to Amazon's arbitration provision. This article spends significant time discussing the critical question of whether the plaintiff's agreement to arbitration related to the subsequent 27 purchases can be retroactively applied to his earlier purchase of the weight-loss product. In the end, it appears the plaintiff didn't challenge that issue, and the Second Circuit Court of Appeals held that he waived the right to do so. --- Nicholas P. Mooney II
