View as Webpage

Issue 2, 2020

The Editors' Note

Welcome to the second 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. In this issue, we take a deep dive regarding the proposed amendment to the North Carolina Identity Theft Protection Act. And then, we look at recent developments stemming from a variety of issues including data plumbing, the CFTC, TCPA, presenting factual information on websites, biometric privacy issues, the U.S. Senate and refusal of cash payments, accessing clipboard data, problems with the SEC, and troublesome facial recognition programs.

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

Proposed Amendment to the North Carolina Identity Theft Protection Act

By Alexander L. Turner

In April 2019, with the introduction of House Bill 904, a bi-partisan effort was made to strengthen cyber security in North Carolina. H.B. 904 seeks to make North Carolina's Identity Theft Protection Act one of the strongest in the nation by broadening the definition of what constitutes a data breach, what proactive steps companies and employers must take to prevent a breach of their customers or employees' personal information, and the penalties available to victims of data breaches, among other provisions.

While H.B. 904 did not make it out of committee and failed to meet the cross-over deadline during the 2019-2020 legislative session, it is anticipated that it will eventually be passed and signed into law if significant federal data breach protections are not passed in the meantime. Therefore, the time for companies that do business in North Carolina, or that otherwise maintain North Carolinians' personal information, to begin preparing for these changes is now.

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

Class Action Alleges Visa-Acquired Co was 'Data Plumbing' Venmo, Cash App & More

"The plaintiffs allege that Plaid violated privacy and data protections by accumulating and monetizing financial transactions of millions of users."

Why this is important: An estimated 50+ million Americans use Venmo to make financial transactions, and an estimated 25+ million Americans use its competitor Cash App. Those applications work by connecting users' banking accounts to fund in-app, peer-to-peer transactions. According to a new proposed class action, however, the company making those connections—Plaid—has misled consumers into believing they were interacting directly with their financial institution when, in fact, they were handing over their log-in credentials to Plaid. The complaint alleges that Plaid then used those credentials to collect years of transaction history from 200+ million accounts, building detailed profiles on its users that helped support the $5+ billion acquisition from Visa earlier this year. Plaid, for its part, disputes the allegations, calling them baseless and denying that it rents or sells user data. The result is yet another front in the battle over big-data practices and consumer privacy. --- Joseph V. Schaeffer

---

CFTC to Develop 'Holistic Framework' for Crypto Assets by 2024

"The CFTC further acknowledged that market regulation needs to keep pace and even lead to encourage responsible innovation."

Why this is important: Regulatory clarity over crypto assets is a ubiquitous topic in this area, with conflicting regulations often leading to uncertainty. The CFTC considers certain crypto assets as commodities, which would place them under the CFTC's jurisdiction. On the other hand, if considered securities, crypto assets would be governed by the SEC. This article discusses the work that the CFTC and SEC are conducting "to really think about which falls in what box" for regulatory purposes. --- Nicholas P. Mooney II

FCC Holds System that Text Platforms Requiring Manual Number Entry are Not ATDS Under TCPA

"This is big news for folks using text platforms that allow template-based, fast-paced texting, on a one-to-one (i.e. click-to-text) basis so long as the phone number is entered each time."

Why this is important: The TCPA generally prohibits a person from calling or texting someone on a cellular phone using an ATDS. The P2P Alliance, a coalition of providers and users of peer-to-peer text messaging services, had filed a petition for clarification asking the Commission to clarify that text messaging platforms requiring a person to manually send each text message one at a time are not subject to the TCPA. On June 25, 2020, the FCC issued a ruling that the TCPA does not restrict text messaging platforms if the platform "is not capable of originating a call or sending a text without a person actively and affirmatively manually dialing each one." In so ruling, the FCC rejected the National Consumer Law Center's position that manual number entry texting platforms enable marketers to spam cell phones, explaining that, "The TCPA does not and was not intended to stop every type of call." --- Tai Shadrick Kluemper

---

In IMDb Privacy Case, 9th Circuit Rejects Hoang's Appeal

"Hoang alleged that IMDb improperly used her personal information to find out her real age and published her real age on its website."

Why this is important: An actress going by the stage name Junie Hoang signed up for the Internet Movie Database ("IMDb") subscription service that allowed her to create a page and display her acting credits. Instead of including her age in the biographical information on her page, she chose to leave that information blank. However, she then used a friend's IMDb account to submit a fake birthdate for herself, making it appear that she was several years younger than she actually is. Not content to be several years younger, she then decided she didn't want the fake birthdate listed, and she began repeatedly contacting IMDb to request that it be removed. IMDb advised it would attempt to verify if the fake birthdate was, in fact, fake. To support her claim that is was a fake birthdate, Hoang submitted several documents, including a fake Texas ID. IMDb wasn't satisfied with the Texas ID (which was fake) and didn't change her listed birthdate (which also was fake). Hoang later sent an e-mail requesting that she be provided with any documents that verified the fake birthdate was accurate. This caught the attention of a customer service manager, who began investigating. Ultimately, he was able to ascertain

Hoang's true birthdate, and the unspeakable then happened. IMDb listed Hoang's correct birthdate on its website. Undeterred, Hoang continued to attempt to convince IMDb that her listed birthdate (which now was accurate) was in fact not, including providing it with a fake passport. IMDb didn't change the information, and Hoang sued it and its parent, Amazon.com, Inc., claiming that the publication of her actual birthdate harmed her employment prospects in the movie industry. This article is significant because it discusses the appeal Hoang pursued after a jury found in favor of IMDb and that the Ninth Circuit Court of Appeals relied on the IMDb subscriber agreement to which Hoang agreed in deciding to affirm the trial court's result. The Ninth Circuit stated that agreement allowed IMDb to do exactly what it did: use the information submitted to its website to improve the accuracy, and the publication of her correct birthdate did not constitute sharing Hoang's confidential information in a manner that the subscriber agreement prohibited. --- Nicholas P. Mooney II

Judge OKs $3.2M Deal to End BIPA Class Action vs Corner Bakery Over Worker Fingerprint Scans

"Under the terms of the settlement, each of the workers would receive about $800, while the plaintiffs' attorneys will reap about one-third of the total settlement funds, minus some administrative costs."

Why this is important: Employers have responded to "punch fraud," the practice where employees punch an absent colleague in or out of work, by adopting biometric time clocks. If employers are not careful, however, they can run afoul of biometric privacy laws where they have been adopted. In Illinois, for instance, the state Biometric Information Privacy Act includes specific standards that a private entity must meet before it can collect biometric information, as well as standards for how a private entity must treat that information once it has been collected. Even procedural violations will give rise to claims, which can cost millions of dollars to resolve. Corner Bakery is just the most recent company to learn this lesson, and wise observers would take from its example the need to closely audit their practices in light of their jurisdictions' biometric privacy laws. --- Joseph V. Schaeffer

---

Bipartisan Senate Bill Would Punish Retailers for Refusing Cash Payments

"Sens. Bob Menendez, D-N.J., and Kevin Cramer, R-N.D., have introduced a bill prohibiting retailers from declining cash payments from customers, as businesses promote 'contactless' digital payment as they grapple with the coronavirus pandemic."

Why this is important: As the world continues to alter its behavior in response to the COVID-19 pandemic, an issue has arisen over the use of cash to make purchases. Some retailers promote "contactless" payments through a variety of digital means as a reaction to the pandemic. A bill introduced in the United States Senate would punish businesses that either refuse to accept cash as payment or charge a higher price for an item if paid for with cash. This article is important because it explains the rationale of the bill's sponsors. Approximately 20 percent of U.S. households have little to no access to bank accounts. Of those, "about 6% are 'unbanked,' meaning they have no access at all." "Fourteen percent of unbanked Americans are Black, 11% are Hispanic and 4% are White." As a result, the sponsors emphasize that refusing to accept cash "discriminates against certain populations and denies people equal access to the same goods or services." If a business refuses to accept cash or charges a higher price for an item if paid for with cash, the bill would provide for a maximum fine of $2,500 for the first offense and $5,000 for the second offense and every offense thereafter. --- Nicholas P. Mooney II

LinkedIn Faces Lawsuit Over Claims It 'Secretly' Read iPhone Clipboard Data

"iPhone user Adam Bauer has sued LinkedIn over claims the job-focused social network 'secretly' read iOS clipboard data often, including the Universal Clipboard that shares copied content with nearby devices."

Why this is important: When Apple announced iOS 14 in June, most users were likely focused on user-interface changes. But some users noticed that Apple added a new privacy setting that lets users be notified when an application reads information from the system's "Universal Clipboard." Armed with this new information, users are fighting back against what they allege is an egregious breach of privacy. A July 10 class-action complaint against LinkedIn, for instance, alleges that the company programmed its

application to read data from the Universal Clipboard—even from other devices on which the application was not installed, and in a way that circumvents Apple's 120-second timeout. The plaintiff alleges that, by accessing Universal Clipboard data, LinkedIn has violated several state and federal statutes, breached its contract with its users, and intruded upon its users' privacy and seclusion. LinkedIn, for its part, issued a statement that its application's access to Universal Clipboard data was a flawed equality check that would be addressed in a future update. For the company, however, the damage has in part already been done—and perhaps most notable is that this is a result of a security decision made by a separate company, Apple, over which LinkedIn has no control. --- Joseph V. Schaeffer

---

In Virtual Hearing, SEC and Kik Lawyers Trade Arguments on Summary Judgment Motions

"At the time, the SEC alleged that Kik 'sold the tokens to U.S. investors without registering their offer and sale as required by the U.S. securities laws.'"

Why this is important: The judicial system continues to become more reliant on technology as society continues to emphasize efficiency and convenience. This trend has only been accelerated by the recent COVID-19 pandemic and the social distancing protocols that have come with it. One such example of the accelerated technology push is a recent virtual hearing that took place in a case involving the U.S. Securities and Exchange Commission and a tech company called "Kik." The subject of the suit involves Kik's recent Initial Coin Offering ("ICO"), which essentially is an Initial Public Offering with Kik's digital currency token called "Kin." The SEC relies on the "common enterprise" theory to contend that Kik's ICO was invalid because it was an unregistered sale of a security. Kik refuted the "common enterprise" theory by stating that all of the investors in Kik experience profits or losses individually, rather than collectively. The way the court rules on this topic could be an influential decision moving forward. Cryptocurrencies are somewhat of novel concept. Although various cryptocurrencies have existed for more than a decade, lawmakers, financial experts, and economists still have trouble determining how to treat it. Most currencies are generated by a government and backed by that government's reserve in something like gold. Digital currencies have no physical form and typically are not generated by a government entity, which leads to ambiguity around its legitimacy. Kik even stated that the SEC's guidance around digital currency sales is insufficiently clear. Whatever clarity the court may provide could set a precedent to either strengthen or weaken the legitimacy of digital currency. As the technology push continues in our economy, digital currency is going to become more and more common. The law is slow to catch up, and the decision in this case could provide some helpful clarity for the continued acceptance of cryptocurrencies. --- P. Corey Bonasso

---

Controversial Detroit Facial Recognition Got Him Arrested for a Crime He Didn't Commit

"But recent uprisings around the country in response to racial injustice in the wake of the death of George Floyd have again brought criticism of the technology to the forefront."

Why this is important: In late June, news outlets across the country reported on what they called the first case of false arrest based on facial recognition software. It turns out, at least one other case preceded it. Another Detroit-area man also was arrested on the basis of a false identification several months earlier in 2019. Although the Wayne County prosecutor's office has responded by limiting the use of facial recognition software to felony investigations, as well as requiring corroborating evidence and a senior-level review of charging decisions, criminal justice and privacy advocates are certain to raise concerns about the practice writ large. In particular, critics of facial recognition software have cited studies showing that the technology struggles to identify persons of color. And many of those same critics have expressed concerns about the use of facial recognition technology to suppress protests and other petitioning activity. Law enforcement, however, argues that facial recognition technology is an effective tool. As facial recognition software expands into civil society, these same debates are set to become much more mainstream. --- Joseph V. Schaeffer

---