SHARE:

Join Our Email List

View as Webpage

Issue 9, 2020

VIDEO: New Developments in the World of Section 230

Nick Mooney and Joseph Schaeffer, Spilman Technology Law Practice Group Chairs, discuss proposed amendments from the Department of Justice, a recent statement from Justice Thomas on the Supreme Court's "shadow docket," and a rulemaking announcement from the FCC.

Vermont Lawmakers Approve Ban on Facial Recognition Technology

"As the Vermont Legislature closed out its session for the year, it passed what is considered the nation's strongest statewide ban on law enforcement's use of facial recognition technology."

Why this is important: The use of facial recognition technology has been a recurring topic in our *Decoded* updates. Beyond the privacy concerns that facial recognition technology presents, advocates for civil liberties and racial justice have raised concerns about its performance distinguishing persons of color. Now, Vermont has taken a significant step toward addressing those concerns by placing a moratorium on law enforcement use of facial recognition technology. With the exception of certain authorized uses of drones, law enforcement is henceforth prohibited from using facial recognition technology, or information acquired through facial recognition technology, until it is authorized by an act of Vermont's General Assembly. This makes Vermont's law among the strongest in the nation and could signal a shift in public tolerance for law enforcement use of facial recognition technology. **---** Joseph V. Schaeffer

Plaid 'Surprised' at TD Bank's Lawsuit Alleging It Tricked Consumers

"Plaid's software includes helping popular apps like Venmo, Coinbase, Square and Stripe access bank and credit card info, and the company says they 'have been working with TD for quite some time, and are disappointed that they resorted to litigation and false allegations.'"

Why this is important: This is the latest allegation against Plaid that it is improperly obtaining and/or selling information relating to millions of customers. In this lawsuit, TD Bank alleges that Plaid used TD Bank's logo and trade dress to make customers believe they were entering personal information into TD Bank's platform when they were actually entering it into Plaid's platform. Plaid denies the allegations and highlighted its history with TD Bank, noting that the two companies "have been working [together] for quite some time." TD Bank's lawsuit isn't the first one to accuse Plaid of improperly obtaining and/or selling information. Earlier reports estimate that Plaid has been alleged to have engaged in similar conduct for several years and that it has affected approximately 200,000,000 individual accounts. --- Nicholas P. Mooney II

Can Hardware Security Modules Lower Your Insurance Costs?

"In 2019, according to industry reports, about 47% of companies with revenues in excess of $1B in annual revenue are currently investing in cyber liability insurance with the adoption rate increasing at about 15% annually."

Why this is important: Companies that have a lot of money tend to want to make sure they don't lose their money. Usually, the larger a company's revenues, the more insurance is necessary. In this era of advancing technology, cyber liability insurance is growing in popularity. Nearly half of companies with annual revenues over $1 billion have some sort of cyber liability insurance policy. If a company with such a policy is the victim of a data breach, these policies can cover things such as lawsuits from people whose data was compromised, fines paid to municipalities, payments to credit-watching agencies, and ransom payments when necessary. Insurance companies don't hand out policies freely, however. As with any insurance policy, the insurer will conduct its due diligence to analyze the level of risk it would be taking on with a given client. A company that has little to no privacy safeguards or data protection protocols in place will pay a higher premium, while a well prepared company with high security will enjoy lower premiums. This type of insurance is relatively new in 2020, but it likely will be a requirement for every major company in the near future. --- P. Corey Bonasso

Supercell to Pay $8.5 Million Over Patent Dispute with F2P Dev Gree

"A patent dispute between two mobile developers has ended in a Texas court ordering Tencent subsidiary Supercell to pay $8.5 million to the Japanese dev Gree for what a jury found to be 'willful' infringement of Gree's patents."

Why this is important: The patents in suit were issued for mobile gaming software including many of the earmarks of "business method patents", which have been difficult to enforce since the case of *CLS Bank International v. Alice Corp*. After *Alice*, many software patents have been declared invalid. The trial court enforced the five patents asserted by Gree, finding them valid and infringed. The jury found that Supercell's infringement was willful, so the trial court may still treble the damages under the patent statute providing for willful infringement. The verdict ($8.5M) is a paltry sum in the context of patent infringement damages generally, but if this amount is ultimately trebled, it may get the attention of other game copycats. Since this is a district court verdict, an appeal by Supercell probably will follow. Gree had previously litigated other patents in Japan and settled with Supercell by licensing more than 1,000 patents for a mere $4.5M. That evidence apparently resulted in the low verdict, as Gree failed to include a nondisclosure provision in its license agreement. --- William P. Smith

Three Million Credit Cards Harvested and Sold on Joker's Stash; Dickey's BBQ Hack Undetected for Over a Year

"Since about mid-2019, about three million credit card data were siphoned off from over 150 of the chain's locations and are currently up for sale on dark web marketplace, Joker's Stash."

Why this is important: How were hackers able to pull off an almost one and one-half year-long data breach to obtain information on three million credit card accounts? It all centers around Dickey's Barbecue Pit, which is the fastest-growing BBQ chain in the country, with more than 150 locations in 41 states. The locations are individually owned franchises, which leaves the owners free to implement

whatever point-of-sale credit card systems they want. Many of them used magnetic stripe systems instead of embedded chip technology. Hackers were able to obtain the financial information and cardholder's information for three million credit card accounts from May 2019 to September 2020. And, despite the length of the breach, Dickey's apparently didn't learn of the breach until the information was advertised for sale on Joker's Stash, a dark web marketplace. At least one commentator maintains that the Dickey's locations aren't blameless. Their use of outdated magnetic stripe technology and the length of the breach lays responsibility at their feet. --- Nicholas P. Mooney II

PayPal Will Soon Let U.S. Users Buy, Sell and Shop with Cryptocurrency

"The company plans to bring digital currencies to Venmo next year too."

Why this is important: PayPal is the latest company to enter the cryptocurrency market and has big plans to promote cryptocurrency use within the United States. Within the next few weeks, PayPal will allow users to buy and sell digital currencies through its platform. Additionally, PayPal intends to help merchants accept cryptocurrency as payment through its service and to facilitate cryptocurrency use in the mobile payment service, Venmo. Finally, PayPal "is preparing for central banks and corporations to set up their own virtual currencies." This is a major step in normalizing cryptocurrency use in the United States. PayPal jumping into the cryptocurrency space also helps cryptocurrency deal with its legitimacy problem, i.e., being perceived as a scam and not being insured by the government. People purchasing cryptocurrency through PayPal are less likely to believe they are being scammed and have an entity from which to seek restitution if an issue arises. Additionally, this will help eliminate some of the money laundering and other criminal activity that is associated with cryptocurrency. Because PayPal is a money transmitter and therefore a money service business, it likely also will be a virtual asset service provider due to the fact that it will settle cryptocurrency payments with merchants in fiat currencies. It is subject to the federal Bank Secrecy Act and therefore must establish procedures to monitor suspicious activity and report it. This step by PayPal could lead to more people using cryptocurrency in the near future. --- Kellen M. Shearin

China Passes New Law Restricting Sensitive Exports

"China has passed a new law restricting sensitive exports to protect national security, allowing Beijing to reciprocate against the U.S. as tensions mount between the sides over trade and technology."

Why this is important: U.S.-based businesses are subject to a host of laws and regulations that restrict the export of sensitive equipment and technology. Now, a new law adopted by the National People's Congress Standing Committee allows China to do much the same within its own jurisdiction. The new law also notably permits China to take "reciprocal measures" against countries or regions that, in its view, abuse export controls in a way that threatens China's national security and interests. Though seemingly intended to provide the legal foundation for retaliation against the United States for its position on TikTok and WeChat—two mobile applications with strong ties to China—the new law has broader implications for global export controls. --- Joseph V. Schaeffer

Biometrics in the Medical Industry is Blooming - What's Next?

"Biometric verification can be a great way to identify the patient and secure the data from unwanted breaches, but is it really enough?"

Why this is important: In 2009, Congress passed the HITECH act, which encouraged healthcare providers to move medical records online by offering incentives to go digital and increasing penalties for HIPAA violations. This created ease of transfer and accessibility to medical records for doctors and patients, but it also made medical information more susceptible to theft by hackers. Personal medical information can be stolen to obtain prescription drugs for use by underage children, drug addicts, or drug traffickers. With access to medical records, fake billing and insurance theft can occur, which can affect both patients and the hospital. Medical identities also are stolen to get treatment under someone else's name to avoid paying for expensive medical bills. Biometric security measures have been one effective combatant against potential hackers. However, hackers also have found ways to impersonate actual

patients in order to bypass biometric security. A proposed solution has been to combine biometric security with Know Your Customer ("KYC") compliance measures. This may be a video call with a patient to verify that the person receiving the information is actually the person to whom the information belongs. This is similar to a two-factor authentication system used by banks, but on a more detailed level. Security for medical information is vital to patient privacy, and healthcare providers must continue to be diligent in their efforts to protect their patients' information. --- P. Corey Bonasso

Ransomware Attack on a Major Health Tech Firm Slows Down Several COVID-19 Clinical Trials

"Targeting clinical trials in the middle of a global pandemic is a new low, even for ransomware operators."

Why this is important: How low is a ransomware attack on a medical technology firm supporting COVID-19 clinical trials? Several companies are asking themselves that question after being subjected to an attack in September. However detestable the attack might be, these risks are now a fact of life, and companies must understand the risk and adapt. In that regard, two points stand out here: first, that health and research data concerning novel coronavirus are major targets for cybercriminals, and even state-sponsored actors, and second, that companies must worry not only about the vulnerability of their own systems, but also those of their vendors. --- Joseph V. Schaeffer

Banks Investing Less in Branches & ATMs and More in Digital

"In what promises to be a boon for fintech, the number of bank branches in the world's developed countries is projected to drop 10% to 30% by the end of 2021."

Why this is important: This article further highlights an issue we've reported on in the past: that is, the effect the COVID-19 pandemic has had on the adoption of financial technology. It's reported that "the number of bank branches in the world's developed countries is projected to drop 10% to 30% by the end of 2021." In fact, this trend already was in process. A study found that the number of bank branches in the United States dropped from 95,000 in 2010 to approximately 83,000 in 2019. The pandemic is expected to accelerate this trend as it has caused more customers to become comfortable with digital banking and all things contactless. Also, although at least one commentator reported on customer preference for in-person banking for more complicated transactions, there's a financial benefit to favoring online banking. The article reports on data comparing the costs to banks for the different types of customer transactions. "The average transaction at a branch costs a bank $5, compared with 60 cents for an ATM, 17 cents for the internet and 8 cents for mobile." --- Nicholas P. Mooney II

U.S. States are Turning to a Private Irish Company to Help Stop the Spread of COVID

"The company's software engineers, who were all used to working remotely even before the pandemic, created COVID Tracker, a decentralized app that keeps users anonymous but alerts them if they've crossed paths with someone who has tested positive for coronavirus in the past two weeks."

Why this is important: An enterprise software company in Tramore, Ireland was thrust into overdrive when the COVID-19 pandemic shut down the world. Software engineers for the company, called NearForm, were all used to working remotely even before the pandemic, and they created COVID Tracker, a decentralized app that keeps users anonymous but alerts them if they've crossed paths with someone who has tested positive for coronavirus in the past two weeks. The massive success of the app has led to the development of similar apps in partnership with NearForm in several U.S. states, with more to come. One factor that has made the company so successful is that the entire process, from building to deploying the app for each new government client, takes less than 30 days, according to NearForm. Development of the app is also cost effective (New York spent $700,000 in partnership with NearForm for its app, while the German government developed its own app for $22.5 million). The app works by delivering anonymous codes via Bluetooth to users who also have contact tracing apps that pass within six feet of a person who was exposed to COVID. The anonymous codes are deleted after 14 days to add privacy. While the app has been hugely successful overseas, the largest hurdle in the U.S. seems to be user adoption. Many Americans are still refusing to wear face masks, let alone download a

contact tracing app. While many hope that the app will gain ground in America, it looks as if there is still a long way to go. --- P. Corey Bonasso

Consumer Reports Study Finds Marketplace Demand for Privacy and Security

"Given the rapid proliferation of internet connected devices, the rise in data breaches and cyber attacks, and the demand from consumers for heightened privacy and security measures, there's an undeniable business case for companies to invest in creating more private and secure products."

Why this is important: Data privacy and security is not just a good strategy for avoiding risk, it is also good business. A recent Consumer Reports study found that 74 percent of Americans were at least moderately concerned about their personal data, with a full 96 percent agreeing that more should be done to protect their privacy. Even more notable is that consumers are willing to pay for privacy, particularly if they've experienced a data breach. And at least one data point suggests consumers might pay a premium: of the respondents who had switched from Android devices to iPhone, 32 percent reported doing so for increased privacy and security. --- Joseph V. Schaeffer

Ensuring the Enforceability of Electronic Arbitration Agreements in Virtual Admission Packets

Alex Turner discusses the risks associated with the use of electronic arbitration agreements and ways that your facility can ensure the enforceability of electronic arbitration agreements.