View as Webpage

Issue 7, 2020

U.S. Judge Halts Trump's TikTok Ban, Hours Before It was Set to Start

"John Hall, an attorney for TikTok, said that the app, with some 100 million American users, is a 'modern day version of the town square' and shutting it down is akin to silencing speech."

Why this is important: These are latest developments in the ongoing feud between the Trump administration and TikTok, ByteDance, WeChat, and TenCent, entities that the administration accuses of stealing information from U.S. users and providing that information to the Chinese government and/or Chinese Communist Party. We discussed in prior issues of *Decoded* the administration's Executive Orders that provided that certain types of transactions with TikTok, ByteDance, WeChat, or TenCent would be prohibited. However, the Executive Orders left it to the Secretary of Commerce to create a list of those transactions, and the list wasn't due until the same day those transactions would be prohibited, leaving virtually no ability for anyone to determine how to comply. Critics charged that the Executive Orders were motivated, at least partially, to hasten Microsoft's talks to purchase TikTok from ByteDance. (Microsoft wasn't successful, but Oracle and Wal-Mart later reached a tentative deal with ByteDance to obtain TikTok.) TikTok and ByteDance sued, claiming the Executive Orders infringed on the First Amendment's free speech protections and due process concerns. Now, a court has sided with them, at least initially. The court has issued an order blocking the Executive Order's prohibition from taking effect. It is yet to be seen what effect this order will have on the ongoing efforts to iron out the remainder of the Oracle-Wal-Mart deal, the separate Executive Order related to WeChat and TenCent, or the lawsuit pending in California over that Order. --- Nicholas P. Mooney II

Judge Temporarily Blocks U.S. WeChat Ban

"In issuing the preliminary injunction, Judge Laurel Beeler wrote that the plaintiffs — a group of US-based WeChat users who stand to be affected by Trump's ban — had shown 'serious questions' in their claim that the executive order threatens the users' First Amendment rights."

Why this is important: A U.S. based group of WeChat users has temporarily succeeded in blocking President Trump's executive order to ban downloads of WeChat. After the WeChat users requested an emergency hearing, U.S. Magistrate Judge Laurel Beeler issued a preliminary injunction finding that the WeChat ban infringed on the users' First Amendment rights and could not survive intermediate scrutiny, a less onerous review of governmental action. Under First Amendment intermediate scrutiny, a Court will determine whether the government's action was narrowly tailored to serve an important government interest. Judge Beeler found that the WeChat ban was not narrowly tailored to serve the government's national security interest because "there are obvious alternatives to a complete ban, such as barring WeChat from government devices" or "taking other steps to address data security." Given reports of the Chinese government censoring WeChat posts that contain criticisms of its President, it is ironic that an American court is using the First Amendment to allow users to continue posting on the platform. This, among other things, is something the Court will have to consider when deciding whether to make this injunction permanent. --- Kellen M. Shearin

---

Dunkin' Data Breach Settlement Paves the Way for More Suits

"Dunkin' Brands' settlement with the New York state attorney general of a lawsuit tied to a five-year-old data breach affecting its Perks rewards cardholders could open the door to suits by other states - as well as customers."

Why this is important: The financial and behavioral information that can be gleaned from consumer loyalty and payment cards isn't just of interest to retailers; it's attractive to hackers as well. This means that retailers who implement those programs can't focus just on their upside, but also must plan for—and protect against—the downside of a data breach. This case is notable because Dunkin Donuts stands accused of having done the opposite—of ignoring its app developer's warnings that it was susceptible to brute-force attacks. It's likewise notable for the consequences, in this case a $650,000 fine on top of monetary refunds to resolve claims affecting just 20,000 consumers in a single state. The lesson here should be that companies collecting consumer data must incorporate data privacy and security from the start. --- Joseph V. Schaeffer

---

Two New Bills in Congress Offer Clarity for Blockchain Tokens and Crypto Exchanges

"The Digital Commodity Exchange Act of 2020 is a bill to this concept that looks to sort out the crypto exchanges who offer the buying and selling of tokens that would fit into the definition provided by Emmer's bill."

Why this is important: Recently, Congress attempted to continue to bring clarity to how crypto assets are classified. The first bill, titled the "Securities Clarity Act," seeks to clarify what is and is not treated as a security in connection with investment contracts. More particularly, the bill would make clear that an asset sold pursuant to an investment contract, whether tangible or intangible (like a crypto asset), that is not otherwise a security, does not become a security merely because it was sold pursuant to an investment contract. The second bill, titled the Digital Commodity Exchange Act, would put cryptocurrency exchanges under the purview of the Commodity Futures Trading Commission instead of making them subject to the money transmitting license procedures of the various states. If these two bills pass, they will be important steps in the ongoing work to develop a clear set of rules that will govern cryptocurrency exchanges and crypto assets in the United States. --- Nicholas P. Mooney II

Warner Music Group Faces Class Action Lawsuit Over Months-Long Hack

"It's unclear exactly how many users were affected by the digital theft, but the legal text notes that 'potentially millions of payment card transactions' were exposed to criminals."

Why this is important: Two plaintiffs filed a lawsuit against Warner Music Group after their banks alerted them to suspicious charges on their credit cards. The plaintiffs discovered that WMG had been the target of undetected hackers over the course of several months. The plaintiffs alleged that WMG did not have adequate safeguards in place to protect its customers' financial information. WMG did not know that the hack was occurring, and the plaintiffs allege that WMG did not give timely notice once the hack was discovered. The ruling in this case could tighten the belts of big companies regarding how they protect their customers' information. If the court finds that the company should have reasonably known that customers' privacy had been compromised, then WMG could be liable for damages to the affected customers, even though WMG had no knowledge that the hack was happening. --- P. Corey Bonasso

---

Biometric Privacy Claim Against Pindrop and Amazon Dismissed for Lack of Jurisdiction

"The putative class action alleged that Amazon had passed voice data from its call center service to Pindrop for conversion into biometric data, but the judge dismissed the charges against both companies on grounds that none of the alleged events took place in Illinois after the plaintiffs had dialed their telephones."

Why this is important: The court's analysis discusses whether individuals in Illinois calling the insurer

John Hancock in Massachusetts was sufficient to confer jurisdiction in Illinois courts. The suit was brought under Illinois' Biometric Information Privacy Act, which exempts John Hancock because it is deemed to be a financial institution. Thus, the suit was brought against Amazon and Pindrop, who were alleged to have captured the callers' data for voice recognition. In finding that Illinois courts lacked jurisdiction, the court noted that neither Amazon nor Pindrop were located in Illinois. Further, there was no indication that either of them purposefully directed their activities to Illinois citizens. Rather, John Hancock had contracted with Amazon and Pindrop to analyze its customers' voices. The only connection to Illinois was the fact that some customers called from there, using their Illinois phone numbers. That, the court held, wasn't sufficient to confer jurisdiction in Illinois courts. --- Nicholas P. Mooney II

Facial Recognition Tech Company Challenges Privacy Class Actions

"Clearview AI, which provides photographic information to law enforcement, faces nearly a dozen privacy class-action lawsuits in New York and Illinois."

Why this is important: Clearview AI, which received national attention when a *New York Times* article uncovered the scope of its facial recognition database, is finding itself in a battle for control over multiple privacy class actions that have since been filed against the company. After an earlier bid at transferring the cases in New York failed before an Illinois-based federal judge, Clearview AI is now trying its luck at coordination before the U.S. Judicial Panel on Multidistrict Litigation. These procedural moves demonstrate the time (and unstated expense) associated with litigating privacy-based claims that, by their nature, can pull in plaintiffs from all across the country. --- Joseph V. Schaeffer

---

In The Future, Your GM Vehicle Might Know You by Your Face

"A new trademark application from General Motors sheds some light on what could be a cutting-edge future comfort control system for cars, trucks, and SUVs."

Why this is important: Many people have experienced the inconvenience of lending a vehicle to a friend only to find the driver's seat and mirrors askew upon return. Given the different sizes and driving preferences of different individuals, it is unlikely that any two people would prefer the exact same settings. Most automakers have addressed this issue to some extent with memory seat buttons, which use motors to reset a driver's seat to previously saved settings. However, this does not help with other settings like mirrors. GM has applied for a patent that could be the beginnings of biometric technology use in its vehicles. Potential uses could be a fingerprint or palm print scanner, or possibly a camera with facial recognition software. These technologies already exist, and GM could be developing vehicles that would offer the ultimate welcome upon entering your vehicle. One could conceivably enter his or her vehicle and it would recognize who the driver is and immediately adjust all settings to that driver's preferences. Seat position, mirror position, music choice, stereo volume, climate settings, and more would be just how the driver likes it without having to press a button. Presumably, this sort of package would come at a premium price if GM's patent is successful and it is the only automaker with this capability. --- P. Corey Bonasso

---

Ransomware Jumps in September as Schools Become Primary Target

"The number of schools hit by ransomware ticked up in September growing to roughly twice the number in August."

Why this is important: The impact of recent increases in ransomware attacks on schools and the effect of some of these attacks is a sign of the times. In some circumstances, the ransomware attacks have completely shut down school's computer systems. The increase in ransomware attacks alludes to the fact that the public sector is gradually reopening, and more people are back to working in schools systems, which means more people are opening e-mails and their attachments. The hacker group Ryuk has a history of attacking schools and is obviously having an impact. Why would schools be a target for such attacks? They're actually considered lucrative targets as they typically have outdated computer systems but also have access to funds to pay a ransom. --- Nicholas P. Mooney II

Twitter Faces Lawsuit by Man 'Doxed' as White Supremacist

"The man was fired after he was publicly linked to a group that espouses racist ideals."

Why this is important: Twitter, and social media generally, can be a rough-and-tumble place. One way this expresses itself is in the form of doxing, a term that refers broadly to the disclosure of a private individual or social media user's personal information. The question here is who, if anyone, is responsible when doxing leads to real-world consequences. The plaintiff, who was fired by his employer after an anonymous Twitter account linked him to a white supremacist organization, argues that it must be not only the Twitter user behind the doxing, but also the user's employer, Twitter, and Twitter's in-house counsel. In reasoning that's reminiscent of some arguments against Section 230, the plaintiff charges that Twitter and its counsel have condoned and facilitated this behavior as part of their opposition to his political views. Until Section 230 is amended, however, the plaintiff's claims against Twitter seem likely to find little headway. Even so, they highlight the difficulty that internet companies face when engaging in content moderation decisions. **---** Joseph V. Schaeffer

---

Tesla Network Goes Down Leaving Drivers Unable to Connect to Their Cars with Mobile App in Massive Outage

"The outage – which appeared to be global – is said to be one of the 'most wide-ranging' in Tesla's history."

Why this is important: Tesla recently experienced an internet outage that spanned the globe. Most vehicles on the road today are becoming more and more dependent on software, but perhaps none more than Tesla. Tesla vehicles rely heavily on software for almost all of their functions, including actual vehicle operation. Driving a Tesla without connectivity could be compared to operating an iPhone without connectivity -- while the device is still functional and aesthetically pleasing, it is incapable of carrying out what it is designed to do. Most people who rely on the internet understand that an outage, even for a short period, is a productivity killer. As society's dependence on technology grows, outages will become more and more of a detriment. Failsafe measures and backup plans will necessarily increase as the potential damage of an outage increases. In this case, Tesla has shown how backups have not yet risen to the necessary level to keep continuous connectivity when a primary connection goes down. --- P. Corey Bonasso

---

Shopify Data Breach by 'Rogue' Employees Exposes Nearly 200 Merchants; Customers Potentially at Risk

"Shopify staff announced that two support team members 'were engaged in a scheme to obtain customer transactional records of certain merchants.'"

Why this is important: In other articles in this issue of *Decoded*, we look at how hackers outside of a business have used various schemes to obtain information or carry out ransomware attacks. As we discussed, businesses need to be on-guard against those attacks. But, businesses also have to be concerned about another kind of data breach, one coming from inside the company. Recently, there was a breach at Shopify where two rogue employees obtained data from approximately 200 merchants and their customers' information. Shopify's response has been swift. It has identified the data that was compromised, communicated with the affected merchants, and is coordinating with law enforcement authorities in their investigation. --- Nicholas P. Mooney II

DOJ to Seek Congressional Curbs on Immunity for Internet Companies

"The Justice Department proposed to Congress ways to curb longstanding legal protections for internet companies such as Facebook Inc., Alphabet Inc.'s Google and Twitter Inc. and force them to shoulder more responsibility for managing content on their platforms."

Why this is important: Section 230, 47 U.S.C. § 230, has facilitated the growth of websites relying on user generated content by allowing those websites to moderate content without fear of opening themselves up to liability. Increasingly, however, Section 230 has come under fire from conservatives, who allege that websites are using its liability protections to discriminate against individuals and topics

associated with conservatives. President Trump acted on those allegations to direct the Department of Justice to evaluate potential reforms. And last week, the DOJ announced its proposed changes—perhaps the most notable of which is to limit Section 230's liability protections for content moderation decisions to those taken in good faith to remove obscene, terroristic, harassing, or otherwise unlawful materials. But given Congress's focus on the COVID-19 pandemic and an intervening election, it is unlikely that Congress will take these proposals up any time soon. --- Joseph V. Schaeffer

---

Patient Breach Victims File Lawsuits Against Assured Imaging, BJC Health

"Pysa ransomware hackers posted patient data from Assured Imaging online, while BJC Healthcare fell victim to a massive phishing attack; the breach victims filed lawsuits in response."

Why this is important: There are two separate lawsuits brought by individuals whose health data was stolen from two different health care providers. In the first hack, the hackers gained access to the provider's system and waited before stealing the data and making the ransom demand. In the second, three of the provider's employees fell victim to phishing attacks. The article discusses the lawsuits brought by the victims whose data was stolen and the claims they are asserting against the providers, including failing to comply with FTC guidelines and minimum industry standards for data security. Health care providers, and anyone who handles sensitive information about third parties, need to take steps to ensure that information is secure from various kinds of cyberattacks and data breaches, which could include ensuring they stay current on any guidelines provided from government agencies. --- Nicholas P. Mooney II
