View as Webpage


Issue 6, 2020

## TikTok Will Partner with Oracle in the United States After Microsoft Loses Bid

*"TikTok and Oracle will become business partners in the United States — a deal meant to satisfy the Trump administration's national security concerns about the short-form video app."*

**Why this is important:** There are developments in the feud between the Trump administration and TikTok's parent, ByteDance. In earlier issues of *Decoded*, we discussed the administration's August 6, 2020 Executive Order prohibiting "transactions" between any person in the U.S. and ByteDance. This led to lawsuits being filed against President Trump, by TikTok, ByteDance, and others. Some commentators believe the Executive Order was aimed at keeping ByteDance's negotiations moving with Microsoft, which sought to purchase TikTok's U.S. operations. It is being reported that a deal has been reached, not with Microsoft, but with Oracle, who will partner with ByteDance in some form. The exact nature of the deal is not yet known, but it has been described as not being an outright sale to Oracle. Also unknown is what effect this deal will have on the Executive Order, the pending lawsuits, and the similar Executive Order issued against TenCent, the parent company of the popular app WeChat. --- Nicholas P. Mooney II

---

## Section 230 and *Doe v. Kik*

*A look into the recent court case, Section 230 and FOSTA.*

**Why this is important:** Section 230(c)(1) of the Communications Decency Act states, "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Professor Jeff Kosseff refers to these as the "Twenty-Six Words That Created the Internet," because they allow websites to publish and moderate user-generated content, such as that found on Facebook or YouTube, without fear of ruinous liability. But these 26 words were also seen as shielding websites that facilitated online sex trafficking, such as Backpage.com, and Congress reacted in 2018 by adopting the Fight Online Sex Trafficking Act ("FOSTA"). As a result of FOSTA, Section 230 was amended to except any civil action brought under 18 U.S.C. § 1595, if it would constitute a violation of 18 U.S.C. § 1591—a statute that prohibits sex trafficking of children. A recent decision involving a lawsuit against the messaging service Kik, however, shows that FOSTA does not open the door to any plaintiff alleging sex trafficking. The plaintiff, proceeding under the pseudonym of Jane Doe, had alleged that Kik users had used the service to solicit sexually graphic photos from her, while also sending her sexually graphic photos of themselves. Doe argued that Kik was aware that its service was being used for this purpose, but failed to take any action to protect her or other minors. But while Doe's complaint alleged the sexual exploitation of a minor, the trial court held that her claim was barred by Section 230 — notwithstanding FOSTA. Central to the trial court's decision was its conclusion that Congress incorporated the "actual knowledge" standard from § 1591 into FOSTA rather than the lesser negligence standard from § 1595. And because Doe could not prove that Kik had actual knowledge of the incidents involving her, her claims fell outside the FOSTA exception to Section 230 immunity. --- Joseph V. Schaeffer

---

## Website Crashes and Cyberattacks Welcome Students Back to

## School

*"Rather than receiving recommendations for best practices and coordinated purchasing plans, districts large and small were largely left on their own while tackling the huge challenge of finding virtual learning platforms and signing contracts within a few months."*

**Why this is important:** The autumn season is at hand, which means students are returning to school. Thanks to the COVID-19 pandemic, the "return" to school is more of a metaphor. Most school districts around the country have resorted to virtual learning platforms to begin the school year. As the reliance on technology has accelerated with the new school year, technical difficulties have increased. Several school districts were delayed by a full day or more, while others had hundreds of thousands of students unable to access their virtual classrooms. The way that the country reacts to this issue could have a major impact on the nation's overall COVID-19 response. Many political leaders have reiterated the importance of education for children. If technical difficulties continue to cause problems for education, the nation's leadership may be forced to weigh the risks of COVID-19 infection against the lack of education for an extended period. The ingenuity of American society likely could rise to the challenge and resolve the technical difficulties, which would allow virtual learning to continue as a suitable substitute for in-person learning. --- P. Corey Bonasso

---

## Fed Partners with MIT Based Digital Currency Initiative to Explore Central Bank Digital Currency

*"The Federal Reserve Bank wants to communicate that it takes CBDCs seriously and is engaged in efforts to research a path toward implementation."*

**Why this is important:** For the past several years, many countries have been developing a central bank digital currency ("CBDC") to act as electronic money. The CBDCs would essentially be the fiat, or government-backed, alternative to cryptocurrencies. Commentators widely hold that the U.S. is behind other countries in the development of a CBDC. Despite lagging behind others, however, the U.S. is working to develop one. An example is the U.S. Digital Dollar Project. This article is important because it discusses other U.S.-based work to create a CBDC, those being the efforts of the Federal Reserve Bank ("Fed") and its recent publication of a paper discussing the role of a CBDC in the future of the U.S. One significant point is the Fed's position that a CBDC "will complement cash, not replace it entirely." The article also discusses the risks that may be inherent in a CBDC, such as increased risks to privacy and illicit activity being conducted with CBDCs. --- Nicholas P. Mooney II

---

## Service of Process Through Social Media Approved by Texas Supreme Court

*"The amendments will take effect on December 31, but public comments submitted to the court until December 1, will be considered if any changes to the amendments are deemed necessary."*

**Why this is important:** Although reports occasionally surface of courts allowing plaintiffs to serve defendants via social media on an ad hoc basis, Texas is the first jurisdiction (to our knowledge) to incorporate service by social media into its rules of civil procedure. Because service by social media is authorized only as a substitute for personal service or service by certified mail, it remains to be seen how frequently it will be used once effective. But we can imagine two circumstances, one obvious and one less so, in which social media service could be particularly helpful. The first is when the defendant is known, but has successfully avoided service by other means—no great surprise there. The second is when the defendant is unknown—perhaps because the individual is known only through an anonymous social media account. In this latter circumstance, plaintiffs might see Texas's approval of social media service as facilitating lawsuits against anonymous social media users. And, if that is the case, Texas might become the go-to jurisdiction for certain types of litigation based on anonymous online behavior. For that reason, Texas's application of this new rule is worth watching. --- Joseph V. Schaeffer

---

## Facebook Class Action Lawsuit Could Pave Way for Biometric Privacy Laws Across the U.S.

*"Combined with the high statutory damages figures made available under the law – ranging between $1,000 and $5,000 'for each violation' of the statute – BIPA is quickly becoming the next privacy class*

*action battleground in the U.S. as attorneys look to cash in on quick paydays that require minimal work."*

**Why this is important:** The Biometric Information Privacy Act ("BIPA") class action lawsuit against Facebook, and the resulting settlement, could lead to an increase in both BIPA class action lawsuits and an increase in legislation targeting biometric privacy. In January of this year, Facebook agreed to a $650 million settlement after the Ninth Circuit ruled that the class plaintiffs had suffered injury from Facebook's violation of BIPA's requirements. Facebook argued that the plaintiffs had suffered no actual harm from a mere violation of the requirements of BIPA, and the district court and the Ninth Circuit disagreed. The Ninth Circuit's ruling put Facebook, and future plaintiffs, in a precarious position in which it may be better to settle than risk paying damages "ranging between $1,000 and $5,000 'for each violation' of the statute." The lawyers of all future plaintiffs bringing a cause of action under BIPA should note this settlement. Due to the sheer size of the settlement, it is likely that plaintiffs' lawyers will use it as "a measuring stick by which to value other BIPA disputes" which in turn could cause settlement values to increase. It also is likely that the increased attention from the Facebook settlement will lead legislators to focus more heavily on passing biometric privacy laws in the 47 states that do not currently have such legislation. --- Kellen M. Shearin

---

## U.S. Sues to Recover Cryptocurrency Funds Stolen by North Korean Hackers

*"U.S. officials said they used blockchain analysis to track down stolen funds from two hacked exchange portals back to the 280 accounts."*

**Why this is important:** This article is important because it relates to one of the most often misunderstood aspects of cryptocurrencies -- that they are anonymous. According to the recent lawsuit filed by the U.S. against 280 Bitcoin and Ethereum accounts, it believes they are holding approximately $2.8 million worth of cryptocurriencies that were stolen by hackers located in North Korea. The U.S. was able to track the funds from the point of being stolen to the accounts now holding them by blockchain analysis. The U.S. essentially tracked every transaction, tracing them as the hackers exchanged the currencies from one cryptocurrency to another (such as exchanging Bitcoin to Etherum to Steller to Tether), a process called "chain hopping," as they tried to cloud the source of the funds akin to money laundering. The funds were frozen by the exchanges before the hackers could convert them into fiat (or government-backed) currency and disappear. Even if you don't want to read the entire article, it's worth taking a look at it to see the infographics of the chain hopping the hackers did when they continually exchanged one cryptocurrency for another. --- Nicholas P. Mooney II

---

## Lessons Learned from the Equifax Data Breach

*"However, the truth is they need to be as comprehensive as they are in terms of the range of security controls needed in order to get anywhere near a state of what could be called secure IT operations.'"*

**Why this is important:** An ounce of prevention, as they say, is worth a pound of cure, and in few places is this more true than in the area of data privacy and security. Data breaches can result in substantial fines and litigation costs, as reflected in the $1.38 billion Equifax settlement that is composed of $1 billion in security upgrades and $380 million in compensation to affected individuals. Equally significant, however, is the reputational damage that comes from being associated with the disclosure of sensitive information, with all the downstream risk that entails for individual customers. But it need not be so. As the security experts quoted in this article attest, there are steps that companies can take now to create systems and, perhaps more importantly, a culture that is protective of data privacy. Given the significant incentives for bad actors to obtain this information, and the substantial consequences if they succeed, their advice is worth heeding. --- Joseph V. Schaeffer

---

## The Future of 'Brain Chip' Technology: Balancing Whether We Can with Whether We Should

*"While you may not know much about brain chips, they are already being used in limited clinical and medical settings to assist people with devastating injuries."*

**Why this is important:** Things that used to be considered science fiction 20 years ago are not so far-fetched today. Today's technological advances are inching very close to the possibility of using a brain implant to control everyday technology such as light switches, appliances, and computers. The electrical

currents that control these everyday technologies are the same electrical currents running through the human brain, and scientists are figuring out how to make them talk to each other. Imagine walking into your home, turning on the lights and music, and flipping on your favorite TV program just by thinking it. Modern technological advances may be close to making it a reality. The practical applications could be largely impactful for victims of serious injuries, quadriplegics, or other physically disabled people. People with physical limitations could supplement their lifestyle with a computer interface linked to their brain. While the advantages are unthinkable, so are the risks. The pessimist in all of us cannot help but think about the dangers this sort of implant could pose. The risk of malfunction is a large factor, but the potential psychological issues abound, as well. When (not if) this technology becomes available for commercial use, the answer may present itself. --- P. Corey Bonasso

---

## Pasco's Sheriff Created a Futuristic Program to Stop Crime Before It Happens. It Monitors and Harasses Families Across the County.

*"In just five years, Nocco's signature program has ensnared almost 1,000 people."*

**Why this is important:** We are living through a time when police are under increasing scrutiny as some call for their defunding and loss of qualified immunity. At the same time, artificial intelligence is being implemented to attempt to improve all facets of our daily lives. These two issues collide as police departments implement AI to increase the effectiveness of their policing in so-called "predictive policing" models. The implementation of AI in this context has taken a few forms. Serious questions are being raised about the form of AI employed by the Pasco County, Florida Sheriff's Department. Some AI platforms break a city or county into segments and review past criminal reports to locate the days, times, and types of crimes that occur within the segments. The platforms then predict that at corresponding days and times similar crimes will occur. Police departments can then deploy officers accordingly to increase presence to try to deter crimes before they occur. Some complain about the biases inherent in this system. That issue isn't decided and still is being debated elsewhere. This article discusses an altogether different way to use predictive policing. In Pasco County, the Sheriff's Department has a team of 20 analysts who review police reports, property records, social media pages, bank statements, and surveillance photos. They then decide what people (not segments of a city or county, but people) are likely to commit a crime in the future. The names of those people are fed into an algorithm that ascribes a score to each person. A person's score can increase every time they have any interaction with law enforcement. The names of those people who reach a certain score level then go on a list, and deputies are dispatched to find those people, question them, determine if there is any basis to write them a ticket or arrest them for anything, and then report back on the number of "prolific-offender checks" they made during their work shifts. Critics focus on what they see as abuses, such as incidents where five patrol cars sat outside one target's home all night, deputies visiting another target as many as six times in a day, deputies visiting another target's mother at her place of employment, and deputies visiting the homes of targets' friends and relatives. Further, if targets' families or friends refuse to speak with deputies, deputies are instructed to look for possible code violations, like a forgotten bag of trash or overgrown grass, as a reason to get the families and friends to talk. On the other hand, some have praised this predictive policing, such as parents of teenage children who have started to have run-ins with law enforcement and who now are receiving heightened attention from deputies in a proactive manner. Similar offender-based predictive policing models are being used in other cities like Chicago and Los Angeles. The issue of the effectiveness and impartiality of predictive policing has yet to shake out, but this article raises concerns about how one police department is implementing AI. --- Nicholas S. Mooney II

---

## Universities Face Digital Accessibility Lawsuits as Pandemic Continues

*"This July and August, digital accessibility suits increased 17 times compared to the first half of the year."*

**Why this is important:** Universities, as well as other places of higher or secondary education, have increasingly become more handicap accessible over recent years. Most buildings, classrooms, and even presentation tools are designed with disabled people in mind. The COVID-19 pandemic has caused most educational settings to move to a virtual platform, which has left some disabled students without proper learning aides. For instance, a hearing impaired person cannot benefit from a presentation without subtitles, and a vision impaired person cannot benefit from a presentation without any sort of audio translation of written materials. Schools that have been focusing on "digital accessibility" before the pandemic are well prepared for this increase in the demand for virtual education. Those who are unprepared will have to catch up to the demand, even after the pandemic subsides enough to allow in-

person learning to return. This is yet another example of the unexpected acceleration of American reliance on technology, which will cause the "kinks" to be worked out on unprecedented timelines. --- P. Corey Bonasso

---

## Rapper T.I. in $75,000 U.S. Settlement Over Cryptocurrency Offering

*"The Securities and Exchange Commission said it had charged the Atlanta rapper and actor along with four associates, including film producer Ryan Felton who it says controlled the companies FLiK and CoinSpark that conducted the initial coin offerings which T.I. promoted."*

**Why this is important:** Cryptocurrency may still be at the cutting edge of financial products and services, but that does not mean that they are wholly outside the existing legal framework. Clifford Harris, better known by his stage name T.I., learned this lesson the hard way after getting wrapped up in a cryptocurrency venture that advertised itself as "Netflix on the Blockchain." Government regulators alleged that Harris violated securities laws when he promoted and sold cryptocurrency in that venture, and Harris paid $75,000 to settle the claims. The lesson here is that consulting with a lawyer before engaging in cryptocurrency ventures can pay dividends down the road in the form of avoided legal problems and fines. --- Joseph V. Schaeffer

---

## Coinberry Crypto Exchange Gets Lloyd's Cover as Canada's Post-Quadriga Rules Tighten

*"Following last year's QuadrigaCX collapse and loss of client funds, Canada's crypto exchanges are going the extra mile to rebuild the trust of consumers."*

**Why this is important:** Canada's cryptocurrency exchanges are obtaining financial institution bonds as a result of the Canadian government's tightening of regulations. What's interesting about this is not the obtaining of bonds, but the government's move to tighten regulations, which commentators attribute to being a result of the recent Quadriga incident. Quadriga embodies the fear that cryptocurrency users have that someone may gain control of their cryptocurrency keys and access their funds. In December 2018, Quadriga's CEO ventured to Asia for vacation, despite the fact that he suffered from what some have characterized as a severe disease. Reports then surfaced that he died. It then was discovered that he was the only person who knew some of the alphanumeric codes required to access Quadriga's customer's cryptocurrencies, leaving those funds inaccessible by others at Quadriga or the customers. Rumors started flying that the CEO had taken the funds, faked his death, and disappeared. It turned out the truth wasn't quite that provocative, but it nonetheless was problematic. The CEO in fact had passed away. Courts employed experts who thus far have been able to recover some, but not all, of the currencies. As more is learned, it appears the CEO had used Quadriga's customers' currencies to fund his expensive lifestyle. The Canadian government has been taking steps to prevent a repeat of Quadriga, and this article discusses one of those steps. The Quadriga saga has been relatively popular in the cryptocurrency world, and this Vanity Fair article is a great place for further reading. --- Nicholas P. Mooney II

---