SHARE:

Join Our Email List

View as Webpage

Issue 10, 2020

VIDEO: Cryptocurrency - Legitimate Uses and Potential Issues

Following the recent publication of the U.S. Attorney General's cryptocurrency enforcement framework, Spilman attorneys Corey Bonasso and Nick Mooney discuss cryptocurrencies, their legitimate uses, and some inherent legal issues, including bankruptcy and tax issues, anti-money laundering requirements, the recent arrests of the BitMEX exchange owners, and the recent $60 million fine to a cryptocurrency mixing service.

The Github Youtube-dl Takedown Isn't Just a Problem of American Law

"It's especially shocking, therefore, when what looks like a domestic legal spat–involving a take-down demand written by lawyers representing the Recording Industry Association of America, a U.S. industry group, to Github, a U.S. code hosting service, citing the Digital Millennium Copyright Act, a U.S. law–can rip a hole in that global development process and disrupt access for youtube-dl users around the world."

Why this is important: Working collaboratively through the coding repository GitHub, an international group of coders has created a script called Youtube-dl that enables the downloading of videos from YouTube. The script is use-agnostic: it can be used for everything from archiving one's own content to appropriating the content of another. It's that latter use case that has the Recording Industry Association of America concerned, and it has served a take-down notice on GitHub demanding the removal of Youtube-dl. In this article from the Electronic Frontier Foundation criticizing the RIAA's action, what is particularly interesting is the discussion of how U.S. law and trade policy drives laws in other, far-flung jurisdictions. Perhaps even more interesting, though, is the thought that a decision on the legality of Youtube-dl under American law could drive the script's availability across the world. --- Joseph V. Schaeffer

NordicTrack Owner Sues Peloton for Allegedly Stealing Bike Features

"Icon claims that two new features in Peloton's Bike+ — a swiveling touchscreen and the bike automatically changing resistance during classes — were 'developed and used by Icon well before Peloton.'"

Why this is important: Peloton has found itself in a legal battle with a company called Icon Health and Fitness, which owns NordicTrack. Icon claims that Peloton has infringed on at least two of Icon's patents for key features of its exercise equipment. Peloton refutes Icon's claims and alleges that Icon is simply attempting to ride on the coattails of Peloton's success. Peloton has had a year of explosive growth with its stock increasing by 360 percent. Peloton's excellent year is partially due to the COVID-19 pandemic. The country closed the doors of numerous businesses, and gyms were some of the first to close and last to reopen. The segment of the population that regularly exercises was forced to look elsewhere for its fitness needs, and Peloton was ready for the demand. However, this is not the first legal battle over patents between Icon and Peloton, nor is it likely to be the last. Peloton's success is another example of how the COVID-19 pandemic has accelerated a trend that was already established. Many Americans are choosing to purchase their own fitness equipment and exercise at home with on-demand fitness programs. Typically, on-demand fitness programs cost far less than an annual gym membership, and they are typically more convenient because no commute is involved. As society begins to shift as close as possible to the "old normal," traditional gyms may have difficulty reaching their pre-COVID levels of success due to the availability of fitness programs over digital media. --- P. Corey Bonasso

Why Deepfakes Could Threaten Everything from Biometrics to Democracy

"Today, deepfake technology is most commonly used to create more realistic fake images or videos, but it can also be used to develop fake biometric identifiers such as voice and fingerprints."

Why this is important: As it turns out "Fake News" is a real thing. Manipulation of photographic images, videos and voice recordings to spread misinformation has never been easier. The repercussions of this technology range from the fairly innocuous (perhaps looking thinner on the holiday card this year) to irreversible harm on a global scale (think manipulation of democratic elections or corporate sabotage). Thankfully, the technology industry is rising to meet the challenge posed by deepfake criminal activity with enhanced face forensic technology, digital watermarking, and other innovations to detect fraudulent biometric identifiers. Businesses moving to biometrics to replace passwords -- stay tuned to deepfake technologies because, as it turns out, the old adage "I can't believe my eyes" has brand new meaning. --- Lori D. Thompson

Cyber Attack Targets Central Florida Orthopedic Patients

"DJO 'became aware that an email account of an All Pro employee may have been compromised as a result of a malicious phishing email scheme.'"

Why this is important: The significance of this data breach story lies in its mundanity. A medical device distributor's employee falls victim to a phishing attack, which exposes the personal information of the medical device manufacturer's clients in the distributor's region. The consequence is an expensive forensic investigation to determine the scope of the breach, negative publicity, and the near-certainty of a lawsuit. The fact is that any company with customer information (and that's every company) needs to take steps to protect against data breaches -- particularly those in the hacker-favorite healthcare and financial services industries. --- Joseph V. Schaeffer

Saudi Twitter Users Grapple with 'Digital Authoritarianism'

"In the following months, separate claims surfaced that a Twitter data breach by Saudi infiltrators in 2015 resulted in a wave of 'enforced disappearances' of regime critics, many with anonymous accounts on the social media platform."

Why this is important: Many of the 12 million Twitter users in Saudi Arabia use the platform to voice opposition to and criticism of the Saudi government. Working through anonymous accounts, they raise concerns over human rights and social justice issues. However, under the guise of what the article describes as "a loosely worded anti cyber-crime law," activists, bloggers, and even royal family members are being imprisoned. Their anonymity has been stripped through a data breach at Twitter and the direct efforts of at least two Twitter employees, who now face charges of spying for the Saudi government. The result was a wave of "enforced disappearances" of regime critics that humanitarian groups charge involves arrests by secret police, imprisonment without access to lawyers, and even killings. --- Nicholas P. Mooney II

U.S. Seizes Virtual Currencies Valued at $24 Million Assisting Brazil in Major Internet Fraud Investigation

"Brazilian authorities estimate that more than $200 million was obtained through this scheme through which more than tens of thousands of Brazilians may have been defrauded."

Why this is important: The United States helped the Brazilian government in its investigation of a large cryptocurrency fraud scheme, entitled "Operation Egypto," by seizing approximately $24 million worth of cryptocurrency. The cryptocurrency seized was owned or controlled by Marcos Antonio Fagundes and was located within the U.S., which is why the U.S.'s cooperation was necessary. A Brazilian court found that Fagundes, and others, solicited investors via the internet and telephone "to give money to the corporations they controlled, in the form of Brazilian currency or cryptocurrency" and then invest that money into various virtual currencies. The court further found that only a fraction of the funds were actually invested in the virtual currencies and "very little was returned to investors." After the Ninth Circuit's opinion in *U.S. v. Hussain*, it will be interesting to see if the U.S. brings charges against Fagundes also. Under U.S. Code §1343, a person is guilty of wire fraud if there if there is a scheme to defraud, U.S. wires are used to perpetrate the fraud, and the perpetrators specifically intend to defraud persons. In *U.S. v. Hussain*, the Ninth Circuit held that the wire fraud statute allowed the U.S. to bring criminal charges against a foreign fraudster if they used U.S. wires to target U.S. citizens. If Fagundes targeted U.S. investors, it is likely that Fagundes' conduct would put him within the ambit of the U.S. wire fraud statute, in addition to the multiple charges already being pursued in the Brazilian court. --- Kellen M. Shearin

Students File Federal Lawsuit Against Indiana University Over Privacy Violations, Breach of Contract

"The suit stems from a 2018 university investigation during which the university searched the student ID card swipe data of students Cameron Gutterman, Dale Nelson, Hunter Johnson and Brian Hiltunen."

Why this is important: The reference to a federal lawsuit over privacy violations suggests that this case has broader implications than it does. In fact, this is a fairly standard Fourth Amendment case in which four fraternity members allege that Indiana University improperly accessed their swipe card data as part of a hazing investigation. But it does highlight just how much data universities have for their students, and how personal some of that data can be. No strangers to privacy requirements given their coverage under the Family Education Rights and Privacy Act, universities also need to be thinking about how to safeguard their students' other data. Failing to do so risks a data breach lawsuit at a time when, between budget cuts and COVID-19 impacts, universities can least afford it. --- Joseph V. Schaeffer

Ongoing Risk Management Failures Bring Major Fines

"Significant fines against big banks serve as important reminders that ongoing failures to correct longstanding compliance and risk management deficiencies will have consequences."

Why this is important: The Office of the Comptroller of the Currency ("OCC") is cracking down on big banks that show an ongoing failure to comply with risk management protocols. Three large banks were all hit with major penalties (Citibank - $400 million; Morgan Stanley - $60 million; and USAA Bank - $85 million) for continued risk management deficiencies throughout the organizations. These large fines are certain to serve as a warning to other major banks or financial institutions that the OCC is beginning to play hardball. Big banks would be prudent to review their current risk management protocols to ensure

that they are adequate and up-to-date to protect their information against existing and new risks. --- P. Corey Bonasso

Moving Beyond Passwords and 2FA

"Could biometrics be the answer to our password woes?"

Why this is important: To date, passwords have played a fundamental role in securing confidential and proprietary information that businesses store electronically, but passwords are not the panacea for data breach prevention. Their efficacy depends on each person proactively protecting his or her password, and such diligence cannot be assumed. Younger generations entering the workforce -- who grew up on electronic devices -- are some of the worst offenders, with 62 percent reporting in a recent survey that they casually share passwords with friends and family, often by unencrypted emails or messaging accounts. Two-factor authentication or "2FA" enhances security but increases user frustration and wastes time. Biometrics may be the answer. Using face or voice recognition in lieu of a password provides a means to increase security while reducing user frustration in the process. Costs of the technology are decreasing, allowing us to visualize a brighter future for data security that is not password protected. --- Lori D. Thompson

Hong Kong Regulator Wants All Digital Currency Exchanges Regulated

"The watchdog previously had an 'opt-in' regulatory framework which it believes has been taken advantage of."

Why this is important: There is another effort to determine the regulatory structure that will apply to digital currency exchanges and the cryptocurrency universe. The long-running issue of what laws and regulations will govern this space has led to a hodge-podge Frankenstein of government rules that sometimes conflict. In the United States, we're turning the corner as regulators implement laws at the federal and state level that bring certainty to this environment. Hong Kong's approach to regulating digital currency exchanges has been different. Traditionally, as long as those exchanges didn't offer securities or futures trading, they were allowed to voluntarily opt-in to regulation or operate outside of regulatory oversight. It isn't hard to see how a voluntary approach to regulation could be abused. Last week, Hong Kong announced that there will be no more opting in to regulation. As of November 3, all digital currency exchanges are being regulated by Hong Kong's Securities and Futures Commission, regardless of whether they offer securities or futures trading. --- Nicholas P. Mooney II

The U.S. Government Seized $1 Billion in Bitcoin from Dark Web Marketplace Silk Road

"The government said it retrieved the roughly 70,000 bitcoins with the help of an unnamed hacker, whose identity is known to the government but who is simply referred to as 'Individual X' in court documents."

Why this is important: Last week, approximately $1 billion worth of bitcoin disappeared from a digital wallet, thought to be linked to Silk Road, without a trace. The FBI shut down Silk Road, a dark website that allowed people to purchase drugs and other illegal goods, in 2013. Elliptic, a firm dedicated to tracking dirty cryptocurrency, noticed the disappearance and initially thought that Silk Road creator, Ross Ulbricht, may have been involved. However, it has been revealed that the United States government was responsible for the disappearance. Sometime in either 2012 or 2013, an unnamed hacker accessed Silk Road's systems and gained access to the cryptocurrency. The hacker agreed to forfeit the assets and transfer them to the U.S. on November 3, 2020. When the U.S. prosecuted Ulbricht, it was left without an answer as to where the proceeds of Silk Road went. This "forfeiture complaint answers this open question at least in part." While the government has recovered $1 billion, there is still more cryptocurrency linked to Silk Road that has not been located. The U.S. has not stated what it will do with the cryptocurrency, but if history is any indicator, it may be sold at auction. If so, investors looking to purchase cryptocurrency should take notice. --- Kellen M. Shearin

PayPal Takes on Bitcoin as CEO Calls Move to Digital Assets 'Inevitable'

"'Our global reach, digital payments expertise, two-sided network, and rigorous security and compliance controls provide us with the opportunity, and the responsibility, to help facilitate the understanding, redemption, and interoperability of these new instruments of exchange.'"

Why this is important: PayPal recently announced it would offer digital currency services for its customers. The announcement sent the value of Bitcoin soaring over $12,500 per coin. The CEO of PayPal said in a statement that he believes a permanent shift from physical currency to digital currency is "inevitable" and is, in fact, already underway. The explicit acceptance and embrace of cryptocurrency by a large financial services company like PayPal is a major event in the world of cryptocurrency. At its inception, cryptocurrency was not widely accepted as legitimate and many associated it with money laundering or other illegal activities. While some illegal activities do occur with cryptocurrency, there are many legitimate and beneficial uses for cryptocurrency. This announcement shows that cryptocurrency continues to become more accepted and legitimate every day. For those who would like to learn more about cryptocurrency and the legal issues surrounding it, please check out our video, which is included with this publication of *Decoded*. --- P. Corey Bonasso

Emulate to Provide FDA with 'Lung Chips' to Evaluate COVID-19 Vaccines

"Initial studies will recreate the natural physiology of specific human tissues and organs in areas where conventional cell culture and animal-based testing methods have limitations, such as Alzheimer's disease and COVID-19."

Why this is important: Animal testing and lengthy, expensive clinical studies before drugs come to market may become a thing of past thanks to Emulate. Using microdevices called "Organ Chips," researchers can predict reliably how the human body responds to medicines, chemicals and foods. Organ Chips are made of clear flexible polymer that contain human cells from a particular organ. The Organ Chip undergoes mechanical manipulation to emulate the microenvironment of the human organ from whence it came, allowing the researcher a birds-eye view of how human tissue reacts to stimuli. The Lung-Chip recreates pulmonary physiology allowing researchers to determine how lung tissue may be destroyed and recovered. Emulate is the holder of the worldwide exclusive license from Harvard University to Organ Chip technology. On October 29, Emulate signed a Collaborative Agreement with the FDA to evaluate COVID-19 vaccines, bringing new hope to individuals and businesses alike that we might indeed resume business-as-usual in the near future. --- Lori D. Thompson

U.S. Federal Reserve, FinCEN Look for Comments on Travel Rule Proposal

"The travel rule requires VASPs or virtual asset service providers, to maintain identity information for every sale/purchase/transfer of digital assets or cryptoassets."

Why this is important: This proposed rule would further impose regulations on digital asset transactions and would reduce the threshold for reporting requirements related to the transfer of funds both in the U.S. and abroad. Under the current rule, financial institutions must collect and retain information related to transfers of funds over $3,000. The proposed rule lowers this threshold to $250 if the transaction involves an international transfer. The proposed rule also would make explicit that the reporting requirement applies to transactions involving convertible virtual currencies and digital assets with legal tender status. --- Nicholas P. Mooney II