SHARE:

Join Our Email List

View as Webpage

March 17, 2021

State of Crypto: It's Time to Talk About NFTs and Intellectual Property Law

"NFTs are all the rage right now, but buyers and sellers should be aware of the different regulatory frameworks that might govern these assets."

Why this is important: NFTs are a hot topic in the world of digital art. A primary question is: Who owns the copyright to the art that is the subject of the NFT? Outside express agreement to the contrary, the copyright will stay with the NFT creator: the artist. The digital nature of the art underpinning the NFT makes duplication extremely easy and a potential minefield for both the artist and the NFT owner. If the artist/NFT creator retains the copyright, the NFT owner owns the art and has the right to display the art, but not to copy or duplicate. With physical art, it is easy to determine if the right to copy and duplicate for commercial reasons is needed; therefore requiring purchase or license of the copyright as well as ownership of the art.

Consider the following scenario. A business has a thriving online presence and wishes to redesign its website to be more aesthetically pleasing. In so doing, the business reaches out to a digital artist for the creation of several unique pieces of digital art to incorporate into the new website. The digital art is created and purchased as an NFT, but there is another concern at play. At how many times and in how many places does the business wish to utilize each NFT for commercial purposes? In this scenario, it would be to the business' advantage to purchase both the NFTs and the copyrights to the underlying works. This would allow freedom to duplicate the art within multiple locations of the business' website and allow the business to develop further commercial uses of the art such as incorporating into electronic newsletters, catalogues, or other publications. It is our standard practice to include in such agreements express work-for-hire provisions, as well as outright assignment of the work and all appurtenant rights. This ensures that the purchaser is not blind-sided by a later realization that they in fact own less than all of the rights they thought they had purchased.

This discussion may seem like conjecture when the current hype is focused on Beeple selling his "Everydays – The First Five Thousand Days" NFT for a cool $70 million. Acquisition of the underlying copyright is not generally a matter of concern primary in the minds of collectors looking to purchase such high value pieces. However, the fast-paced change to an increasingly digital world means that NFTs could very well be here to stay. Mark Cuban certainly seems to think so. If NFTs are to become part of the norm, then there is good reason to look ahead to the underlying legal issues, which are a necessary, if less glamorous, part of commercial transactions for artistic works. --- Brandon M. Hartman

Twitter CEO Jack Dorsey has Created an NFT for the First Tweet

"Dorsey has become a cryptocurrency proponent, and as such it's not a surprise he's riding the NFT wave by 'minting' the tweet on the blockchain."

Why this is important: NFTs are the new darling of the technology and art world. That's no surprise when creators can easily monetize their digital works, and collectors can acquire them to enjoy or turn around for a quick return on investment. What is surprising, however, are the types of things that are being turned into NFTs and then sold. The first tweet might be an interesting historical artifact, for example, but is it really collectible? And even if it is, does it really merit the current bid of $2.5 million? The best answer probably is that art and value are all in the eye of the beholder. But it also seems fair to say that at least some of the drive to create and sell NFTs is a type of digital gold rush, with creators and speculators both rushing to get in on the ground floor. As with any gold rush, the real question is how long it will last before the value has been extracted and the market stabilizes. --- Joseph V. Schaeffer

---

BitMEX Executive Surrenders in New York, Pleads Not Guilty

"Delo and fellow BitMEX executives Arthur Hayes, Samuel Reed, and Greg Dwyer are accused of operating an unregistered trading platform and violating U.S. anti-money laundering laws by providing unlicensed services to U.S. citizens."

Why this is important: We've written in earlier issues of *Decoded* about the legal troubles of BitMEX. Among other things, it is being accused of operating a cryptocurrency exchange in the U.S. without complying with Know Your Customer and Anti-Money Laundering regulations. It gained fame after receiving notice of the U.S. investigation and its CEO remarking that BitMex was located in the Seychelles, instead of the U.S., because it could bribe local authorities for as little as a coconut. Since then, one member of the BitMex executive team has been arrested. This article reports on the surrender of another executive and the anticipated surrender of a third. Still another is refusing to surrender. The important point is that complying with Know Your Customer and Anti-Money Laundering requirements are, or at least should be, commonplace in cryptocurrency exchanges now. The wild west days of the exchanges have ended, or at least are ending. --- Nicholas P. Mooney II

Chinese Hacking Spree Hit an 'Astronomical' Number of Victims

"A single group appears to have infiltrated tens of thousands of Microsoft Exchange servers in an ongoing onslaught."

Why this is important: Microsoft Exchange servers, the backbone of many organizational communication systems, have been infiltrated on a massive scale. The Chinese hacking group known as Hafnium has breached accounts on a global scale. When Microsoft identified the vulnerability and released a patch, Hafnium automated the hacking to increase the speed at which it could hack before the patch was widely implemented. Besides the breach itself, the hack left behind a web-shell, essentially a backdoor access point, in these servers, preserving access until the foothold is removed. Unlike the SolarWinds mass hack, discovered only a few months ago, this attack appears to have been caught and patched relatively early in the attack's widespread campaign. The contrast between these two incidents showcases the importance of having data privacy and cybersecurity protection in place, frequent monitoring to detect breaches early, and the pivotal significance (the importance of which cannot be stressed enough) of frequently updating all software for the latest patching. --- Risa S. Katz-Albert

---

New COVID-19 Vaccine Candidate Leveraging Nanotechnology is 'Promising'

"Researchers from Cleveland Clinic's Global Center for Pathogen Research & Human Health, who have developed the nanotechnology based vaccine, say it has shown strong efficacy in preclinical disease

models."

Why this is important: Nanotechnology plays the critical role in development of another COVID-19 vaccine. Relying on the SARS-CoV-2 protein that binds with a specific target on our cells in order to penetrate and spread, this new vaccine will use nanoparticles found within almost all living organisms to carry and deliver weakened fragments of this same protein to trigger an immune response. An important benefit of this vaccine will be that the biomaterial comprising it does not require strict temperature control, therefore easing transportation and storage needs. Further testing is necessary to verify the thermostability of the vaccine. So far, this vaccine has shown promise in animal trials and researchers aim to begin clinical trials soon. **---** Brandon M. Hartman

---

Fitbit's First Product Since Being Acquired by Google is Just for Kids

"The wrist-worn device is designed to encourage kids to get moving, with steps and activity tracking via animated clock faces featuring bunnies, rocket ships, and other cartoonish designs."

Why this is important: Google says that it has found a way to use technology to limit the use of technology. Huh? In January, Google acquired Fitbit for the low price of $2.1 billion, and last week, Fitbit announced that its first new product of 2021 is a Fitbit made just for kids -- the Ace 3. This wearable fitness band is designed to get kids off their phones, computers and controllers and get kids moving by doing all the things that Fitbit does so well -- counting steps, reminding when it's time to stand and move, and tracking activity. Minions, cartoons and cute animal designs will make kids want the newest $80 "tech" gadget on their wrist until they get hooked (like the rest of us) on hitting their daily fitness goals. The irony that the technology giant is marketing technology designed to reduce the use of technology is not lost, but Google gets creativity points for disguising its true mission. Google found a whole new market of empty wrists (about 74 million between the ages of 6 to 18 in the U.S. alone) that are about to be filled -- with new technology. --- Lori D. Thompson

---

Hackers Stole NFTs from Nifty Gateway Users

"Some people who were hacked also said their credit cards on file were used to purchase additional NFTs, also costing thousands of dollars, which were then transferred away to a hacker's account."

Why this is important: NFTs have exploded in popularity in recent weeks, especially after an NFT of digital artist Beeple's Everydays: The First 5000 Days sold at Christie's for a staggering $69 million. It seems like everywhere you look, people are talking about NFTs, whether it's news of Twitter CEO Jack Dorsey minting the first tweet into an NFT or a debate about the ecological impact of NFTs. Attention and money are moving into this space like never before. It's easy to understand why hackers would be drawn to NFTs. Now, Nifty Gateway, an NFT marketplace, has announced that several users have had their accounts hacked. The culprits stole users' NFTs and also used credit information on file to purchase additional NFTs that they transferred out of the users' accounts. Nifty Gateway was quick to note that its platform was not breached and that all of the affected users failed to have two-factor authentication enabled on their accounts. Thus, as the credentials were valid, it theorizes the hackers obtained the information from leaks on other platforms. This article highlights two realities. Take basic steps, such as two-factor authentication, to protect your accounts. And, whenever you're drawn to a new, exciting space to invest your money, realize that hackers are drawn to it, too. --- Nicholas P. Mooney II

New McDonald's Drive-Thru is Using AI Technology to Take Orders, Make Suggestions

"The AI technology takes the order, while human employees can focus on accuracy and quality."

Why this is important: AI technology is omnipresent. It's built into the iOS and Android software that powers millions of smartphones. It powers online chatbots and 800-number phone trees. And now, it's taking orders at McDonald's. Though the article focuses on AI opening up human employees to focus on accuracy and quality, it is hard not to be suspicious that the announcement was timed to coincide with discussions about a federal minimum wage hike. But whether there is movement on a minimum wage increase or not, the implementation of AI in these contexts seems inevitable. They don't require training,

they don't require payment, and they don't require breaks. What is less clear, however, is how consumers will respond. Will they miss having their order taken by a human? Will AI systems adapt to regional and foreign accents? And, what will be done with the data? These latter questions are particularly relevant, because other AI systems—facial recognition systems, in particular—have been subject to legal challenges on the basis of discrimination and the misuse of private data. It will be interesting to see if this type of AI system will be subject to the same fate. --- Joseph V. Schaeffer

---

TikTok Agrees to Pay $92 Million to Settle Data Breach Lawsuits

"The proposed settlement has been called one of the largest privacy-related payouts in history."

Why this is important: After more than a year of legal battles, the video-sharing App TikTok has settled numerous lawsuits consolidated into one multi-district litigation suit alleging violations of data sharing policies and laws after sharing user data with several third parties, including some based in China. At $92 million, this marks one of the largest privacy-related settlements (though it pales in comparison with Facebook's $650 million settlement in 2020), and money isn't the only thing to come out of these negotiations. TikTok has agreed to cease collecting biometric information (like facial recognition data) or access the App users' GPS location data. Seeing how TikTok complies with the settlement agreement requirements will be something to watch, as they had been cited and fined in early 2019 by the Federal Trade Commission for similar allegations relating to the collection of information about underage users. --- Risa S. Katz-Albert

---

This is the Year that CRISPR Moves from Lab to Clinic

"In 2021, we will discover even more uses for the innovative gene-editing technology."

Why this is important: 2022 will mark the 10th anniversary of the discovery of the CRISPR-Cas 9 process of genetic editing; a discovery that is deemed one of the most significant in the history of biology. Here, one of the co-inventors of the CRISPR gene-editing tool provides a snapshot of the advances made to date utilizing this technology and highlights several of the next advancements to expect from this technology. From improved detection of viruses to individualized therapeutic treatments to addressing sustainability and security issues in the global food chain, real-world applications of CRISPR-based solutions will soon bring widespread and rapid changes to the lives of millions. The next decade will bring even more CRISPR-derived advancements to bear against many of the problems facing our world today. --- Brandon M. Hartman

---

At Dubai Airport, Travelers' Eyes Become Their Passports

"But the efforts also have renewed questions about mass surveillance in the federation of seven sheikhdoms, which experts believe has among the highest per capita concentrations of surveillance cameras in the world."

Why this is important: Getting through the airport has never been easier in the United Arab Emirates. Starting last week, it takes only five or six seconds to get through check-in, but that short-term convenience will have long-term implications where privacy is concerned. On March 7, the UAE launched use of its iris scanner technology to check in passengers at Dubai's airport, which is the world's busiest airport for international travel. The technology eliminates the need for human contact in the check-in process, which is great for curbing the spread of the coronavirus -- but consider how that technology works. The UAE is reputed to have the highest per capita concentrations of surveillance cameras in the world, resulting in what is reputed to be the largest facial recognition database in the world controlled by the UAE government. Now, the Dubai immigration office is tying the information already within that facial recognition database -- to the information provided by domestic and international passengers when they fly -- to their iris biometrics, which is far more reliable than a facial recognition scans can ever be. The biometric privacy statement given to passengers when they participate in the iris scan is vague as to how their personally identifiable information will be stored and utilized by the UAE government, stating only that it will be retained for "as long as it is reasonably necessary for the purposes for which it was collected." Last month, the UAE Prime Minister announced that its facial recognition technology will be utilized in "some private sector services," but did not disclose what that means and to whom the information will be made available. Under normal circumstances, an invasion of privacy by a foreign

government would face significant international scrutiny, but in the time of pandemic, it is unclear who is watching as an ever-increasing amount of personal data is gathered. The UAE has touted its web of surveillance cameras as a useful tool in the battle to control the spread of the virus by utilizing thermal cameras and face scans to detect whether masks are worn and even to take temperatures. The question that should be on the minds of international community is what becomes of all the information on international travelers that has been tied together and is currently being stored somewhere in Dubai and controlled by the UAE. --- Lori D. Thompson

---

IRS Initiates 'Operation Hidden Treasure' to Root Out Unreported Crypto Income

"Operation Hidden Treasure, a joint effort between the IRS' civil office of fraud enforcement and its criminal investigation unit, will train agents to look at blockchains to root out tax evasion among cryptocurrency users."

Why this is important: Carolyn Schenck, national fraud counsel for the IRS Office of Chief Counsel, sent a message to people using cryptocurrency to engage in fraudulent and tax evasion activity. "We see you." Schenck is leading Operation Hidden Treasure, a "joint effort between the IRS' civil office of fraud enforcement and its criminal investigation unit." The task force is developing "signatures" that it will use to examine blockchains to identify these transactions. Activities that may pique the IRS' interest include structuring multiple transactions so the value of the transaction falls below the reporting requirement and using shell corporations to conceal money. Additionally, people who get "on and off the chain" may be subject to the IRS' scrutiny. On chain transactions are simply transactions that happen on the blockchain. Off chain transactions involve an agreement made outside of the blockchain and can be structured so that the cryptocurrency ownership changes without alerting the blockchain. With anonymity being one of the main features attracting some people to cryptocurrency, it will be interesting to see what happens once people realize that the IRS can see what they are doing. --- Kellen M. Shearin

---

The Accellion Breach Keeps Getting Worse and More Expensive

"What started as a few vulnerabilities in firewall equipment has snowballed into a global extortion spree."

Why this is important: When Accellion, a file sharing platform, first notified customers of a zero day vulnerability in January 2021, most of its customers stopped using the Accellion systems. However, for some customers, the damage had already been done. Flagstar Bancorp, a bank headquartered in Michigan, was one of those Accellion customers. Flagstar notified its customers on March 6, 2021 that while they had responded promptly to the notification from Accellion, there had already been a significant compromise to their files. While details are still under investigation, the timing of this issue has brought frustration from bank clients. Situations like this highlight not only the need to ensure your internal privacy and cybersecurity systems are up to snuff, but also the critical importance of vetting your contractors to ensure their compliance with laws, regulations, and industry standards. --- Risa S. Katz-Albert

---

High-Speed 3D Printing Method Takes Us One Step Closer to Printing Organs

"The new method uses stereolithography and jelly-like materials known as hydrogels to speed up the process."

Why this is important: Researchers at the University of Buffalo have developed a technology that is many times faster than industry standards for 3D printing, which could prove to be a central part of the production of 3D printed human tissues and organs. In a proof of concept test, a full human hand model was printed in 19 minutes. Conventional 3D printing methods would normally require approximately six hours for the same task. This new method, called stereolithography, is deemed particularly suitable for printing cells with embedded blood vessel networks -- yet another crucial piece of the puzzle for 3D printing human tissues and organs. **---** Brandon M. Hartman

---

Twitter Sues Texas AG, Claiming Retaliation for Trump Ban

"Federal lawsuit alleges Paxton is seeking to punish Twitter for taking Trump's account offline."

Why this is important: Conservative politicians have been complaining for years that social media companies have exhibited a liberal bias and discriminated against their speech. So when Twitter and several other social media companies suspended or removed then-President Trump's accounts in the wake of the January insurrection, some of them unsurprisingly took this as proof positive of their claims. Texas Attorney General Paxton took it even one step further, announcing an investigation into Twitter for its decision. But as these social media companies have long pointed out, their moderation decisions are not subject to the First Amendment standards that apply to the government. At the same time, though, the social media companies benefit from those protections—like anyone else in America—when it comes to government efforts to compel or stifle speech. So what's interesting here is that Attorney General Paxton's "free-speech" investigation might put him at odds with the First Amendment. Because similar efforts to Attorney General Paxton's are playing out in conservative legislatures across the country, how the First Amendment question is resolved here could have far broader consequences, making this a case to watch. --- Joseph V. Schaeffer

---

Crypto Project PAID Exploited, Attacker Gains Over 2,000 ETH After Minting Nearly $160M in Tokens

"Network data shows that just over 2,000 ETH -- worth roughly $3 million at press time -- was obtained by the attacker after some of the 59.7 million minted PAID tokens were traded on the decentralized exchange service Uniswap."

Why this is important: This type of attack may be unknown to some people in the cryptocurrency space and also is one of the consequences people may not consider. Paid Network, a decentralized finance app that uses blockchain technology, has reported that an "infinite mint" attack has occurred. Because of the way the token was programmed, an infinite number of tokens could be created. Someone has done just that, creating an extra $180 million worth of PAID tokens. The resulting suspicion of the token has crushed its price, making it drop around 85 percent. Discussion is rampant on the internet that it was an inside job. Regardless of whether it was, two things are clear. There are an infinite number of cryptocurrencies and tokens on the market today. You should ensure you understand how a currency or token operates before becoming involved with it. Also, when a currency or token in which you're involved is hit by a hack, even if your account wasn't compromised, you may still suffer a loss. --- Nicholas P. Mooney II
