View as Webpage

Issue 1, 2020

Welcome!

Welcome to the inaugural issue of *Decoded* , Spilman's e-newsletter focusing on technology law, including data security, privacy standards, financing technologies, and digital-based means of conducting business. When it comes to technology and the law, the bottom line is this: businesses risk everything if they fail to keep up. This is why Spilman has formed a multidisciplinary team of attorneys to assist clients with these issues. And, it's why we have developed this e-newsletter--to help keep our clients and friends informed of the ever-changing landscape of technology law.

Our goal is to provide you with something unique in *Decoded* --namely, timely and insightful information from our attorneys on the top technology law news stories. As with any of our publications, we appreciate your feedback. If there is a certain area or industry you would like to hear more about, please let us know. Likewise, if you think we should send this e-newsletter to your friend(s) or colleague(s), or if you would like to be removed from this mailing, please email us .

We hope you find this information useful and look forward to your feedback. Thank you for reading.

Spilman Thomas & Battle Technology Practice Group

Tech Group Files First Lawsuit Challenging Trump's Social Media Executive Order

"The Center for Democracy and Technology's lawsuit accuses the Trump administration of singling out Twitter for punishment and seeking to 'chill the constitutionally protected speech of all online platforms and individuals.'"

Why this is important: On May 28, 2020, President Trump signed an Executive Order on Preventing Online Censorship. In recent years, conservatives have alleged their viewpoint is being censored by various social media platforms. As the executive order recognizes, those platforms are the "21st century equivalent of the public square." The question becomes whether those platforms can censor viewpoints with which they disagree without running the risk of incurring liability based on the content they publish. More specifically, the executive order aims to determine whether the Good Samaritan protection against liability in Section 230 of the Communications Decency Act is being expanded too far when used by social media platforms as a protection when they edit and moderate content their users publish. The executive order directs agencies to study the way in which this protection against liability is being used and determine whether federal advertising dollars are being spent on platforms that censor certain political viewpoints. The executive order directs the Federal Trade Commission to determine whether federal laws, such as provisions prohibiting unfair or deceptive acts or practices in commerce, would support action against those who are censoring and directs the Attorney General to work with the states to determine if state laws prohibit this type of censorship. A few days later, on June 2, 2020, the Center for Democracy & Technology, an advocacy group funded by technology companies, filed a lawsuit against President Trump in federal court in D.C. seeking a declaration that the executive order is unlawful and invalid as violating the First Amendment's freedom of speech and an injunction against the President from any actions to enforce the executive order. With the filing of this lawsuit, the battle is in motion to

determine whether social media platforms run the risk of incurring liability when they censor viewpoints with which they disagree or whether any attempt to stop them from doing so is an impermissible violation of their First Amendment rights. --- Nicholas P. Mooney II

The ACLU Sues Clearview AI, Calling the Tool an 'Unprecedented Violation' of Privacy Rights

"The ACLU alleges that Clearview's technology runs afoul of the 2008 Illinois Biometric Information Privacy Act, according to the complaint."

Why this is important: Clearview AI made headlines earlier this year when news reports disclosed its creation of a "faceprint" database that could identify millions of people using photos from the internet. Now, it is facing a lawsuit from the ACLU and other organizations, which allege that Clearview's faceprint database violates the Illinois Biometric Information Privacy Act ("BIPA"). That law was adopted in 2008 as a first-in-the-nation approach to protecting biometric information, including facial geometry. And it contains three requirements before that biometric information can be used: (1) written disclosure of the fact of collection and storage; (2) written disclosure of the purpose and length of the collection, storage, and use; and (3) a written release by the subject. The plaintiffs argue that Clearview has not complied with any of these requirements, and they criticize as insufficient the company's voluntary measures, which include excluding photographs with Illinois geotags from its database. They thus ask for a court order requiring Clearview to destroy all unlawfully collected biometric information and come into compliance with BIPA on a going-forward basis. Beyond the novel issues involving faceprint technology, the lawsuit highlights the risks of a uniform approach to data privacy in a regulatory environment where multiple standards can apply. --- Joseph V. Schaeffer

---

Quadriga was a Ponzi Scheme, Ontario Securities Regulator Says

"OSC, one of Canada's provincial securities regulators, said the now-defunct cryptocurrency exchange, which went into bankruptcy a few months after founder and CEO Gerald Cotten was reported to have died in India, 'was an old-fashioned fraud wrapped in modern technology.'"

Why this is important: Quadriga, called "something like TD Ameritrade for cryptocurrency" by Vanity Fair, was at one time Canada's leading Bitcoin exchange. Like an online stockbroker, investors could deposit currency into it and buy Bitcoin. On December 9, 2018, news reports began surfacing that Gerald Cotten, Quadriga's CEO, had died while on vacation in India. Shortly thereafter, some news outlets reported that Cotten alone held the passwords to access Quadriga's (investors') funds and those passwords died with Cotten. Thus, the funds were inaccessible - lost. About this same time, some began questioning whether Cotten really had died or whether his death was an elaborate con to allow him to take the funds and abscond to sunny beaches. Quadriga filed bankruptcy. Creditors lined up. The court appointed experts, like Ernst & Young, to try to maximize the amount of funds that could be returned to investors. All of this sounded like a big cautionary tale to investors, whether in traditional stocks or cryptocurrencies, and it was. But, the Ontario Securities Commission's report added another chapter to the cautionary tale. It reported that, prior to his death (of course), Cotten set up fake accounts in other exchanges in order to use his investors' funds for his own investments, failed to maintain records, opened accounts under aliases, and credited himself with fictitious account balances which he then traded with his own investors. It also revealed that the earlier reports that the funds were lost because Cotten took the passwords with him to the grave were not true. Instead, he simply lost the funds through his "fraudulent conduct." The importance of this story, and the entire Quadriga saga, is in remembering that we still are in a period where the cryptocurrency markets are not as regulated as other investments and the financial markets. Any investment involves trust in a third party. That trust becomes even more important here as one of the hallmarks of cryptocurrencies generally is the immutability of transactions. Generally speaking, once a transaction is made, it can't be undone. --- Nicholas P. Mooney II

'The Computer Got It Wrong': How Facial Recognition Led to False Arrest of Black Man

"What makes Williams' case extraordinary is that police admitted that facial recognition technology, conducted by Michigan State Police in a crime lab at the request of the Detroit Police Department, prompted the arrest, according to charging documents."

Why this is important: ACLU's lawsuit against Clearview AI, which alleges that "faceprint" databases could be used to target protesters, was filed just two days before mass protests over George Floyd's death broke out on the weekend of May 30, 2020. Just weeks later, the dystopian prediction came true when Detroit police arrested a Black man based on a mistaken "faceprint" match. Although ultimately charges were dropped and the man was released, the incident is certain to increase scrutiny over the use facial recognition technology. And given that current facial recognition technologies have been shown to more frequently identify people of color than white people, government and private business should be particularly cautious about the contexts in which they are applied. --- Joseph V. Schaeffer

---

Digital Dollar Project Releases White Paper on US CBDC

"The white paper posits that if the US dollar is to remain the world's primary reserve currency, it cannot remain an analog instrument and unit of account for assets increasingly denominated as digital tokens."

Why this is important: The Digital Dollar Project seeks to encourage public discussion on the benefits of the U.S. creating a digital dollar. Similar to digital currencies/cryptocurrencies like Bitcoin, Ethereum, Monero, and others, the U.S. Digital Dollar would exist in electronic format. However, unlike those others, the Digital Dollar would have the backing of the U.S. government and, thus, would be considered a type of Central Bank Digital Currency (as opposed to a digital currency created by someone other than a government). The Digital Dollar Project argues that a U.S. CBDC will promote individuals' privacy rights while simultaneously allowing increased compliance and regulatory processes. It also promises that, like other digital currencies, a Digital Dollar could increase the speed with which money is transferred while reducing costs. Finally, it admits that, in its viewpoint, the creation of a Digital Dollar is required to "future-proof" the dollar and keep the U.S. at the forefront of financial innovation. The U.S. isn't the only or first country to experiment with the creation of a CBDC. Dozens of other countries have been working to create their own CBDC for the past couple years. Interestingly, some of those countries argue that they need to create their own CBDC to foster their country's inclusion in the global money markets and to avoid trade restrictions by the U.S. --- Nicholas P. Mooney II

ACLU Argues GPS Tracking in LA Violates Scooter Riders' Rights

"'There are better ways to keep rideshare companies in check than to violate the constitutional rights of ordinary Angelenos who ride their vehicles,' said Mohammad Tajsar, senior staff attorney at the ACLU Foundation of Southern California."

Why this is important: This is another battle in the war over the privacy implications of anonymized data sets. The City of Los Angeles and the Los Angeles Department of Transportation (together, LA) have been collecting data from dockless scooter trips using their Mobility Data Specification ("MDS") software. Although anonymous, the plaintiffs argue that it requires relatively little effort to associate the MDS data with individual users. Repeated trips between residential and office locations, for instance, might allow LA to match an employee with his or her place of work. And perhaps more ominously, the MDS data might allow LA to identify individuals who engaged in protests or other petitioning activity. The plaintiffs allege that this violates their protections against unreasonable searches and seizures under the federal and state constitutions. And because MDS could set a precedent for other forms of transportation, such as ride-sharing applications and autonomous vehicles, the plaintiffs suggest a particular urgency for resolving these issues now. --- Joseph V. Schaeffer

---

This NBA Player has Something to Sell You: His Contract

"NBA players have been investing their money in businesses for decades, but this year one player is aiming to flip that model. Brooklyn Nets point guard Spencer Dinwiddie wants you to invest in him, and he plans to use blockchain technology to make it happen."

Why this is important: A recurring theme in the blockchain and tokenizing arena is the concept of removing brokers and putting power in the hands of the performers. Brooklyn Nets point guard Spencer Dinwiddie is taking that concept to the NBA. Last year, Dinwiddie came up with an idea to attempt to turn his contract into a vehicle for digital investment. In essence, he would sell digital shares of his contract. At first, the NBA denied his request, claiming that the way it was structured violated their collective bargaining agreement. Earlier this year, Dinwiddie was able to get an agreement that would let

his plan move forward. Dinwiddie created a company, DREAM Fan Shares, a blockchain investment platform, that would sell 90 shares in his contract for $150,000 each to verified accredited investors under SEC Regulation D, Rule 506(c). The benefit to Dinwiddie is that he's paid the full amount of his contract now instead of waiting the three years of his contract. The benefit for investors is that they stand to be paid interest monthly and receive a full pay out when the investments mature in 2023. Ultimately, if Dinwiddie's plan is successful, it may pave the way for other performers to mimic this structure or create their own in search for ways to take more financial control over the contracts and careers. --- Nicholas P. Mooney II

Attorney General Mark Brnovich Files Lawsuit Against Google Over Deceptive and Unfair Location Tracking

"Arizona has brought forward this action under the Arizona Consumer Fraud Act to put a stop to Google's deceptive collection of user data and obtain monetary relief up to and including forcing Google to disgorge gross receipts arising from its Arizona activities."

Why this is important: The State of Arizona's lawsuit over Google's location-tracking practices would be notable for its target alone. But one of the specific allegations merits particular attention: Arizona argues that it is enough under its consumer fraud statute for Google's privacy settings to have been "confusing and misleading." The implication is that it is not enough to give users control over their location data; the control must also be presented in a way that a consumer can comprehend. At present, Arizona has simply presented a theory based on an allegation. Proof and a legal ruling lie somewhere down the line. But other businesses relying on consumer consents to location-sharing should sit up and take notice, and then revisit their disclosures to ensure they are comprehensible to the average user. --- Joseph V. Schaeffer

---