View as Webpage

Issue 4, 2020

Crosmun v. The Trustees of Fayetteville Technical Community College Provides Much Needed Guidance to NC Courts on How to Properly Craft eDiscovery Protocols

By Alexander L. Turner

The Court of Appeals decision in *Crosmun* is important because it finally provides guidance to North Carolina courts on how to properly craft electronically stored information protocols while still preserving privileged and confidential information and documents.

Click **here** to read the entire article.

Sen. Merkley Introduces Bill Limiting Corporate Use of Biometrics

"The 'National Biometric Information Privacy Act of 2020' would prevent private companies from collecting individuals' biometric information, such as eye scans, faceprints, fingerprints, and voiceprints."

Why this is important: Few topics in data privacy are receiving more attention at the moment than the use of biometric information. Now, Senator Merkely (D-Ore) and Senator Sanders (I-Vt) have introduced legislation that would limit private companies' collection and use of biometric information without individuals' consent. Like the Illinois Biometric Information Privacy Act ("BIPA"), with which it shares many similarities, the draft legislation would limit private entities' ability to collect biometric information for purposes of providing a service or for some other valid business purpose, and then only with the individual's informed written consent. The draft legislation also would obligate private entities to adopt a written policy for retaining and destroying biometric information, with destruction mandated after the reason for its collection has been satisfied or the individual has failed to interact with the private entity for more than a year. And like BIPA, the draft legislation would create a private cause of action with financial penalties for non-compliance. --- Joseph V. Schaeffer

---

Fintechs are Moving Into Bitcoin, but Expect Crypto Startups to Stay on Their Home Turf

"The list of financial technology companies that have jumped on the crypto bandwagon continues to grow."

Why this is important: This article is important because it explains how some fintech companies, such as Square and SoFi, have "jumped on the crypto bandwagon" and enjoyed, in some instances, large profits as the popularity of cryptocurrencies continues to grow. The article uses Square as an example and explains how its prematurely released second quarter earnings show that it made $875 million in bitcoin revenue with its Cash App. That equated to $17 million in gross profit during the same period. --- Nicholas P. Mooney II

Evil AI: These are the 20 Most Dangerous Crimes that Artificial Intelligence Will Create

"The participants were asked to rank the list in order of concern, based on four criteria: the harm it could cause, the potential for criminal profit or gain, how easy the crime could be carried out and how difficult it would be to stop."

Why this is important: A group of scientists from University College London ("UCL") compiled a list of 20 AI-enabled crimes based on academic papers, news and popular culture, and expert opinions on the subject. The list utilized four factors as to the severity of each AI-enabled crime: (1) the harm it could cause, (2) the potential for criminal profit or gain, (3) how easy the crime could be carried out, and (4) how difficult it would be to stop. Based on these factors, the consensus for the most serious AI crime was deepfakes. Deepfakes use fake audio and video to impersonate another person. A creator of an effective deepfake video could make it appear as if any person was saying anything the creator chose. For example, a person could create a deepfake of the President of the United States declaring war on any other nation or perhaps a CEO of a major company denouncing a certain protected class of people. One major issue, which may be the most concerning, over deepfakes is the impact on the population. Rather than false stories spreading and causing confusion, the end result likely will be a widespread distrust of audio and visual content. Without a valid and reliable method of authentication, dissemination of important information through visual and audio methods would be rendered ineffective. --- P. Corey Bonasso

---

Macy's Hit with Privacy Lawsuit Over Alleged Use of Controversial Facial Recognition Software

"The lawsuit, which is seeking class-action status, was filed in Chicago federal court on behalf of Isela Carmean, a regular Macy's customer whose image was likely identified — without her consent — through a facial recognition database, the complaint alleges."

Why this is important: In May, the ACLU sued Clearview AI over that company's software that creates profiles for individuals using photos and other data from the internet. Now, a Chicago woman is suing Macy's over that company's use of the Clearview AI software to monitor its customers. And though the claims under the Illinois Biometric Information Privacy Act ("BIPA") are typical, it is notable that the alleged liability stems from Macy's use of third-party software—thus showing that companies cannot avoid litigation risks by simply relying on software created by others. --- Joseph V. Schaeffer

---

Facebook is Getting More Serious About Becoming Your Go-To for Mobile Payments

"Facebook is aiming for a more cohesive strategy around digital payments with the formation of a new division, Facebook Financial, that 'will run all payments projects, including Facebook Pay.'"

Why this is important: This article is important because it discusses Facebook's recent creation of a new division called Facebook Financial. This division will manage all of Facebook's payment projects, including Facebook Pay. The goal is to keep more users in Facebook's platforms when purchasing items or transferring money instead of those users jumping into other apps and platforms, such as PayPal, Venmo, Apple Pay, and Google Pay. Currently, in the United States, it is available for use in Facebook, Messenger, and Instagram, but in other parts of the world, it's currently only available in the core Facebook app. --- Nicholas P. Mooney II

Class-Action Lawsuit Claims TikTok Steals Kids' Data and Sends It to China

"Twenty separate but similar federal lawsuits were filed over the past year on behalf of TikTok users in California, where the company has offices, and Illinois, which requires that technology companies receive written consent before collecting data on a person's identity."

Why this is important: Even before President Trump issued an executive order targeting TikTok and its parent company, ByteDance, over national security concerns, a group of plaintiffs were alleging that TikTok was harvesting their private information—including draft videos that they discarded without posting—and then sending it to China. And whether that allegation is true—something that TikTok has denied—both the lawsuit and President Trump's executive order highlight the tight-rope that multinational companies often walk when conducting operations in a foreign jurisdiction. --- Joseph V. Schaeffer

---

51% Attack Bleeds More than $5M from Ethereum Classic

"Forensic analysis suggests the recent Ethereum Classic blockchain reorganization was a carefully orchestrated malicious attack."

Why this is important: This article is important because it discusses that a recent split in the Ethereum Classic ("ETC") blockchain actually resulted from a 51% attack. Broadly speaking, a 51% attack occurs when an individual or group controls 51 percent or more of a cryptocurrency's computing power. When they do, they have the ability to stop transactions from being confirmed and thereby added to the blockchain record of transactions. They also are able to, in essence, reverse transactions, which would allow them to spend the same cryptocurrencies twice, in other words, double spending those currencies. This article discusses how a hacker rented computing power from a third party at a cost of approximately $192,000 to gain control over the ETC network. After doing so, the hacker was able to confirm transactions in a certain order that allowed approximately $5.6 million in ETC being double spent. --- Nicholas P. Mooney II

Zoom Encryption Claims False, Watchdog Alleges in Lawsuit

"A Washington, D.C.-based watchdog group is the latest to sue Zoom Video Communications over allegedly false privacy protection claims, saying the company misled and deceived users, such as those in the health care industry, who expected that the technology's encryption would protect their personal information."

Why this is important: A watchdog group based out of Washington, D.C. has sued Zoom, alleging that the company's claims that it utilized end-to-end encryption are false. The complaint discusses several claims that the encryption method used in Zoom's technology is secure enough to be in compliance with HIPAA when used by medical professionals. The COVID-19 pandemic has created a corporate environment within the United States that requires an alternative to face-to-face communication. Zoom has stood out as a platform with a user-friendly interface that allows both video and audio communication among multiple users. These features have made it one of the most popular, if not the most popular, alternative to in-person meetings. Due to the increased usage, the findings of the court could have a particularly drastic effect on the national corporate environment. Attorneys using Zoom may have assumed attorney-client privilege was protected. Doctors using Zoom may have assumed they were complying with HIPAA. If these assumptions proved to be misplaced, major liability issues could arise for those unwary professionals whose communications were not protected. --- P. Corey Bonasso

---

Lawmakers Urge 'Proactive Policy' for Taxing Digital Currency Staking Rewards

"A number of congressional lawmakers have written to the Internal Revenue Service, urging a proactive policy for taxing digital currency that avoids hampering proof of stake technology."

Why this is important: This article is important because it discusses the recent letter by a number of members of Congress to the IRS arguing that the taxing of cryptocurrency staking rewards as income may overstate a taxpayer's actual gains from participating in staking and discourage people from participating in this activity. Staking is used in cryptocurrencies that operate on a Proof of Stake, instead of Proof of Work, model. In the Proof of Work model, like Bitcoin, miners compete to solve complex mathematical problems. The first to do so is given the right to add the next block of transactions to the blockchain record of transactions. By contrast, in a Proof of Stake model, users agree to lock up a certain amount of their cryptocurrencies, or stake them, in order to have a shot at being assigned the right to validate the next block of transactions. The user who is assigned that right is then rewarded with staking rewards. Currently, those rewards are taxed as income, but the letter to the IRS Commissioner argues a more fair way is to tax those rewards when they are sold. --- Nicholas P. Mooney II

Instagram Faces Lawsuit Over Illegal Harvesting of Biometrics

"In the new lawsuit, the company is accused of collecting, storing and profiting from the biometric data of more than 100 million Instagram users, without their knowledge or consent."

Why this is important: Facebook is once again the target of a claim alleging that the company harvested users' biometric data in violation of the Illinois Biometric Information Privacy Act ("BIPA"). An Illinois resident alleges that Facebook's Instagram subsidiary creates facial-recognition profiles from uploaded photos and then uses the data to match users across Facebook services. While this claim might not be unique, the plaintiff's basis for bringing it is: the plaintiff alleges she only learned that her biometric information was being collected from a disclosure the company was required to file under California's Consumer Privacy Act ("CCPA"). If this signals a trend of CCPA disclosures prompting privacy litigation, then companies will need to take an even harder look at their disclosures and data privacy practices going forward. --- Joseph V. Schaeffer