Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

May 12, 2016

BITCOIN/VIRTUAL CURRENCY

NYS Approves Gemini Trust Company to Trade Digital Currency Ether

The New York State Department of Financial Services has approved the application of Gemini Trust Company to trade the digital currency ether on its platform, which is the first time the state has consented to the trading of a digital currency that is not Bitcoin.

Ether is a token or digital asset from the Ethereum platform, a blockchain platform, which includes a public ledger of all ether transactions. It uses ether to execute peer-to-peer contracts without the need for intermediaries.

Gemini Trust Company began trading ether on May 9, 2016. It is reported that ether is the second largest virtual currency behind Bitcoin and has continued to increase since its start in 2015.

— Linn Foster Freedman

CYBERSECURITY

Auto Parts Manufacturing Company Joins Auto Industry Cybersecurity Sharing Group

We have previously reported on the efforts of the auto industry to become more aware of and address data security issues with smart cars [view related posts here and here].

Delphi Automotive PLC has announced that it will join the Automotive Information Sharing and Analysis Center's information-sharing group (ISAC).

Since the design and development of car parts is crucial to the vehicle's security, the addition of Delphi, one of the largest auto parts manufacturers in the world, into the group makes a lot of sense.

According to the chair of Auto-ISAC, the addition of Delphi in the ISAC "will help the industry continue to produce more advanced vehicles with modern and robust security protections incorporated from conception."

— Linn Foster Freedman

DATA PRIVACY

Waze App Vulnerable to Driver Tracking

In the category of being careful with location-based services when using apps, researchers at the University of California-Santa Barbara have discovered a vulnerability in the popular Waze app that permitted them to create “ghost drivers” that could monitor drivers in the vicinity and track them in real time.

Basically, the researchers were able to intercept communications between Waze and users’ phones by getting the phones to accept their computers as the connection between Waze and the users and could then reverse-engineer the Waze protocol. The researchers were then able to write a program that allowed them to create thousands of “ghost cars” and “ghost drivers” that could monitor the drivers around them.

The head of the research team exclaimed that “it’s such a massive privacy problem.” Other recent complaints since Waze updated its app in January is that when a user downloads it, it requests access to all of your contacts. Not sure why it needs your entire contact list to help you navigate from point A to point B. Just a reminder to read those pop-ups when you download an app.

— Linn Foster Freedman

Notice of Proposed Rulemaking, Exemption for Biometrics Database from the Grasp of the Privacy Act

Last week, the U.S. Department of Justice (DOJ) issued a notice of proposed rulemaking in the Federal Register moving to exempt the FBI’s biometrics database from the notice and consent provisions of the Privacy Act of 1974 (Privacy Act). The Privacy Act governs the collection, maintenance, use, and dissemination of personally identifiable information (PII) that is held by federal agencies. The Next Generation Identification (NGI) System (i.e., the FBI’s biometrics database) is supposed to build upon the fingerprint database currently held by the agency by linking multiple forms of biometric data (such as iris scans, palm print and facial recognition data, and personal and biographic data). The proposed rule suggests that the NGI System should not be subject to the restriction from sharing information without the individual’s consent because it would undermine the agency’s ability to carry out its work.

The DOJ said, “Providing access [to individuals whose information is disclosed] could compromise sensitive law enforcement information; disclose information which would constitute an unwarranted invasion of another’s personal privacy; reveal a sensitive investigative technique; could provide information that would allow a subject to avoid detention or apprehension; or constitute a potential danger to the health or safety of law enforcement personnel, confidential sources, and witnesses." The DOJ additionally requests that the “necessary and appropriate” data collection limitation set forth by the Privacy Act be waived because “it is not always possible to know in advance” what types of information may be relevant to law enforcement.

The DOJ also contends that it takes “seriously” the obligation to maintain accurate records, and it will share information with individuals or waive the exemptions “in appropriate cases.” The DOJ’s Privacy and Civil Liberties Office will be accepting public comment through June 6, 2016.

— Kathryn M. Rattigan

HEALTH INFORMATION

Joint Commission Lifts Ban on Physicians Texting Patient Orders

The Joint Commission, which is the national accrediting organization for health care organizations, has long banned physicians using text messages to place orders for patient care due to data security concerns. In 2011, the Joint Commission stated that texting was not acceptable for health care providers to text orders for patient care, treatment, or services.

This month, in its *Perspectives* magazine, the Joint Commission admitted that it had performed additional research concerning the issue and has concluded that the security in texting platforms have become more secure, and therefore, it lifted the prohibition.

In doing so, it acknowledged that texts can be secure with certain platforms, and therefore, as "long as healthcare organizations implement one of these platforms and include the required components of an order, orders can be transmitted through text messaging."

The requirements include a secure sign-on process, encrypted messaging, delivery and read receipts, date and time stamp, customized message retention time frames, and a specified contact list for individuals authorized to receive and record orders.

The texting of the orders must comply with the requirements of the Medication Management Standard for a complete medication order and, obviously, must comply with the Security Rule of HIPAA.

Although the Joint Commission lifted the ban, health care entities should have an organizational process in place before health care providers start texting away. There are specific requirements that must be followed so the texts can be integrated into the patients' medical record in a compliant way.

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

Uber Hit with Class Action Case for Sending Political Texts to Customers

Uber Technologies, Inc., was hit with another class action lawsuit [view previous post] last week for allegedly violating the Telephone Consumer Protection Act (TCPA) when it sent text messages to its customers without prior written consent.

The suit, filed in federal court in Texas, alleges that Uber sent text messages to its customers to urge them to oppose mandates proposed by the City of Austin to require that Uber perform background checks on its drivers. The texts have been dubbed "political" by the plaintiffs, which they allege are prohibited by the TCPA.

— Linn Foster Freedman

Caribou Coffee Faces TCPA Class Action for Unwanted Text Messages

Caribou Coffee Co. Inc. (Caribou Coffee) was hit with a class action this week in Wisconsin, which alleges that the company violated the Telephone Consumer Protection Act (TCPA) when it sent unsolicited text messages to thousands of individuals who never consented to receive those text messages. Lead plaintiff, Kristie Farnham, alleges that she received over 50 text messages from Caribou Coffee advertising their product. Farnham is seeking fines of either $500 per message (if negligently sent) and $1,500 per message (if knowingly sent in violation of the TCPA). Farnham estimates that the class of individuals affected by Caribou Coffee's TCPA violations could be "in the tens of thousands."

— Kathryn M. Rattigan

Intermedix Data Breach Class Action Case Dismissed

We previously reported that Intermedix was sued in a class action lawsuit regarding the data breach involving millions of patient records [view related post].

On May 3, 2016, the parties to the suit agreed to dismiss the case with prejudice, with no payment of attorneys' fees, costs, or other expenses to the other party, which means that each party is to bear its own costs. There is no mention of a payment amount to settle the claims.

— Linn Foster Freedman

Credit Protection Association Settles FCRA Violations for $72,000

A debt collection agency, Credit Protection Association (CPA), settled with the Federal Trade Commission (FTC) this week for its violations of the Fair Credit Report Act (FCRA) for $72,000. In the FTC's complaint, the FTC said that CPA failed to follow the Furnisher's Rule of the FCRA by not having policies and procedures in place to handle consumer disputes; it did not have a policy in place to notify consumers of the outcomes of investigations as required by the FCRA; and CPA failed to inform consumers whether their information had been corrected after a dispute had been received. Director of the FTC's Bureau of Consumer Protection, Jessica Rich, said, "Companies that fail to live up to [the FCRA] obligations can expect to hear from the FTC." In addition to paying $72,000 in civil penalties, CPA will also be required to put the appropriate policies and procedures in place to ensure compliance with the FCRA. There is no mention of a payment amount to settle the claims.

— Kathryn M. Rattigan

Facebook Biometric Class Action Continues in California

A federal district court in California recently rejected Facebook's request to dismiss a class action lawsuit related to Facebook's biometric facial recognition database. The case arises from a complaint by Illinois residents that Facebook's "Tag Suggestions" program violates the Illinois Biometric Information Privacy Act (BIPA) [view related posts here, here and here]. When a Facebook user uploads a photograph, the program scans the photograph for identifying features, suggests names for the faces in the photograph, and encourages Facebook users to tag the individuals who have been named. Illinois is one of a handful of states in the U.S. that regulates the use of biometrics and facial recognition technology.

In the suit, the plaintiffs allege that the Tag Suggestions program violated BIPA because Facebook did

not inform users that biometric identifiers were being created, collected, and stored; describe the purposes for the use and how long the data would be stored; provide a publicly available retention schedule or guidelines for permanently destroying the identifiers; or receive a written release from the plaintiffs to collect or otherwise obtain their biometric identifiers. While the case originated as three separate cases in Illinois, the parties agreed to move them to federal district court in California and consolidate them into one class action. Facebook argued that California law should apply, as that is the law designated in its user agreement. The court rejected that argument, noting that California does not have a biometric policy similar to BIPA, and therefore, if California law were to apply, it would override Illinois' policy of protecting its citizens' biometric data. Facebook is also challenging whether the images collected actually fall within the scope of BIPA. The court did not rule on that issue stating that "those questions are for another day."

— Pamela H. Del Negro

FTC Issues New FCRA Guidance for Employment Background Screening Companies

The Federal Trade Commission (FTC) issued new guidance for employment background screening companies containing information on how to comply with the Fair Credit Reporting Act (FCRA). One of the key elements of this new guidance is information related to when a company's work defines it as a "consumer reporting agency" under the FCRA. This guidance also outlines requirements for background checks and dealing with clients, as well as how to interact with consumers. Check out this helpful new guidance to stay on top of your company's obligations.

— Kathryn M. Rattigan

DRONES

FAA Announces Advisory Committee and More Ease for Students to Operate Drones

Last week, Federal Aviation Administrator (FAA),Michael Huerta announced the establishment of a broad-based drone advisory committee. The creation of this committee stems from the successful stakeholder-based unmanned aircraft systems (UAS) registration task force and the MicroUAS aviation rulemaking committee. However, unlike other committees, this advisory committee is intended to be "long-lasting" according to the FAA. The advisory committee will "identify and prioritize integration challenges and improvements and create broad support for an overall integration strategy." The CEO of the Intel Corporation, Brian Krzanich, will chair the committee.

Additionally, Huerta announced that the FAA will soon permit students to operate UAS for educational and research purposes. This means that schools will no longer need to apply with the Section 333 exemption, and faculty will be able to use drones as well to help students with their courses. Huerta said, "Schools and universities are incubators for tomorrow's great ideas, and we think this is going to be a significant shot in the arm for innovation."

— Kathryn M. Rattigan

FAA's Drone Detection Initiative

This week the Federal Aviation Administration (FAA) expanded its Pathfinder Program by signing the Cooperative Research and Development Agreements (CRDAs) with Gryphon Sensors, Liteye Systems, Inc., and Sensofusion to add to the detection and identification of unmanned aircraft systems (UAS)—or drones—that are flying too close to airports. FAA senior advisor on UAS integration Marke Gibson said, “Sometimes people fly drones in an unsafe manner. Government and industry share responsibility for keeping the skies safe, and we’re pleased these three companies have taken on this important challenge.” These three companies will contribute to the Pathfinder Program by utilizing technologies that have the ability to detect, track, and identify "errant or hostile" drones in and around airports across the country. The new technologies introduced by these companies will be used at FAA selected airports. Check out more information on the Pathfinder Program here.

— Kathryn M. Rattigan

Maritime and Space Industries Testing Unmanned Aircraft Technology for Surveillance

In response to the migrant crisis in Europe, the European Space Agency and the European Maritime Safety Agency have selected the unmanned aircraft system TEKEVER for testing the benefits of deploying unmanned aircraft for surveillance, including search and rescue missions. This is being touted as the first demonstration of drone technology being used for maritime surveillance operations. The testing will commence this summer.

During the testing, TEKEVER will be deployed from land and will assist with determining how the deployment of unmanned aircraft can augment or replace satellites, manned aircraft, and vessels.

The testing will take place in the Atlantic Ocean, the North Sea, and the Mediterranean Sea during multiple environmental conditions.

— Linn Foster Freedman

INTERNET OF THINGS

Sony to Patent Smart Contact Lens

If you don’t wear contacts now, you may want to start thinking about wearing some if (and when) Sony patents and releases its smart contact lens. Sony has officially filed a patent for smart contact lenses which would allow the ‘user’ the ability to record and play back video. The patent references the ability of the lens to connect wirelessly to your smartphone, and allow you to flick through different commands by blinking your eye, such as taking photos. Yes –with a blink of your eye. The lens will be able to differentiate between the conscious and unconscious blink of your eye by the duration of the blink. But what could a camera in your contact lens possibly be able to do? Well, Sony says that it will have the ability to adjust the zoom, focus and aperture.

Additionally, because the lens features a built-in storage unit, the ‘user’ will be able to play back videos on its own display screen so you can view moments of your life simply by closing your eyes.

The patent has not yet been reviewed, so the actual availability of this lens is not yet certain. We are not even sure how much of the technology actually exists at this point. But Sony isn’t the only one filing these type of patents. Last month, Samsung and Google had similar patents up their sleeves. The privacy implications for this product are vast; if you could record a conversation or enter a facility that holds proprietary information or trade secrets without anyone knowing you are actually recording what you are

viewing, it could become a very big problem. We will see what the future has in store.

— Kathryn M. Rattigan

DIGITAL ASSETS

Digital Assets…Coming Soon to a State Near You!

In the hours leading up to the legislature's constitutional adjournment deadline of midnight on Wednesday, May 4th, the Connecticut State Senate passed House Bill 5606, the "Connecticut Revised Uniform Fiduciary Access to Digital Assets Act." The bill, passing unanimously on the consent calendar, extends a fiduciary's existing authority over a represented person's assets to include such person's digital assets. Section 3 of the bill defines a fiduciary as (1) executor or administrator of a deceased person's estate; (2) court-appointed conservator of a protected person's estate; (3) agent appointed under power of attorney; and (4) trustee.

The bill establishes the processes a fiduciary must follow to gain access to a represented person's digital assets, including items such as email, digital photos, electronic documents, music, and social media accounts. Specifically, a fiduciary must send a written request to the custodian along with (1) a certified copy of the document granting fiduciary authority, such as a letter of appointment, court order, or certification of trust; and (2) certain other information the custodian requests, such as account verification. A custodian must generally comply with a request within 60 days and is immune from any liability for an act or omission done in good faith compliance.

In addition, a user, through an online tool, may direct a custodian to allow or limit access to a designated person. The "online tool" is defined as an electronic service provided by a custodian that allows a user, in an agreement separate and distinct from a general service agreement, to provide directions for disclosure or nondisclosure of digital assets to a third person, including a fiduciary. A direction regarding disclosure through an online tool overrides a contrary direction in a will, trust, power of attorney, or other record if the online tool allows the user to modify or delete the direction at all times.

House Bill 5606 replaces the narrow provisions under current law that require email service providers to give estate executors and administrators access to, or copies of, the email account of a decedent domiciled in Connecticut when he or she died.

The bill, effective October 1, 2016, now awaits Governor Dannel P. Malloy's signature.

— Scott N. Siedor

FINANCIAL PRIVACY

European Banking Authority Contemplates the Use of Consumer Data by Financial Institutions

In order to better address both the opportunities and risks associated with the innovative use of consumer data by financial institutions, the European Banking Authority (EBA) released a discussion paper last week seeking public comments on the subject.

The EBA notes in the paper that the increasing digitalization of the economy and the adoption of computing technology that is able to draw inferences from seemingly unrelated sets of data "is generating a new wave of opportunity for economic and societal value creation." By using "big data," financial

institutions are able to offer cost-effective targeted advertising, more accurate credit-worthiness assessments, and better financial advice to their consumers. Consumers benefit from lower costs, enjoy precise insight into their financial situation, and are potentially better protected from fraud. As an example of fraud protection, the EBA points out that a financial institution that knows where a consumer lives, where she normally shops, what she typically buys, and the amounts she routinely spends is better able to spot a fraudulent transaction, protecting the consumer against financial loss.

However, the innovative use of consumer data by financial institutions also presents new risks. The EBA notes that the potential for data theft and identity fraud is ever present as financial institutions continue to gather more and more specific consumer data. Consumers may also be harmed when financial institutions sell data to third parties or rely on inaccurate data to make financial decisions. Even absent any malicious misuse of data, "consumers may be hindered from choosing a different provider for the provision of financial services" if financial institutions do not allow for the portability of consumer data, resulting in consumers being "locked-in" to their relationship with their financial institution.

The EBA notes a number of additional opportunities and risks presented by the innovative use of consumer data by financial institutions.

— Norman H. Roos and Scott M. Baird

DATA SECURITY

PCI DSS Version 3.2 Contains Substantial Changes for Payment Card Processors and Their Service Providers

In April 2016, the Payment Card Industry Security Standards Council published a new version of the PCI Data Security Standard (PCI DSS). PCI DSS Version 3.2 is intended to emphasize the importance of validating the existence and testing effectiveness of security controls for parties in the payment card collection and processing chain. The changes are essentially in two areas, those that apply to primary parties and controls for service providers designated under the PCI-DSS Standard.

For primary parties, the most significant change relates to multifactor authentication. Previously, PCI DSS required untrusted, remote access into systems that are part of the cardholder data environment to use two-factor authentication. Under PCI DSS 3.2, multifactor authentication is required for users with 'administrator' access to the cardholder data environment. The change to the term "multifactor" recognizes that organizations may choose higher security standards. The more important aspect of the change is that internal systems require re-architecture to provide multifactor authentication as part of the authentication process. This means that a password will no longer be enough to verify most user's identity and grant access to the systems in scope of the Standard.

Service providers, as designated under the Designated Entities Supplemental Validation (DESV) appendix to the PCI DSS Standard, have a new set of requirements. The new requirements include maintaining a documented description of the service provider's cryptographic architecture, reporting on failures of critical security control systems, and formalizing executive management responsibility for protection of cardholder data and the PCI DSS compliance program. Entities that are not designated service providers, but may touch on a part of the overall cardholder environment, are recommended to comply with the DESV as well.

The new requirements under PCI DSS 3.2 are considered best practices until January 31, 2018, at which time they will be mandatory.

— Richard M. Borden

DATA BREACH

Wendy's Confirms Data Breach of Point of Sale System

Wendy's confirmed yesterday in its first quarter financial statement that its investigation into a credit card breach did uncover malicious software on its point of sale systems on fewer than 300 of its stores nationwide [view related posts here and here]. It further confirmed that the malware has been removed from the affected locations.

The malware is believed to have been installed through third-party vendor credentials starting in the fall of 2015. We have seen many examples of this over the past two years, which emphasizes how important it is to manage third-party access to systems.

— Linn Foster Freedman

PRIVACY TIP #34

Get Women on Your Board—They Are More Attuned to Risks Facing the Organization

As a member of Women in the Boardroom, I am a big supporter of adding more diversity, including women, to corporate boards.

Now I have a new reason. According to the 2016 Global Board of Directors report, a collaboration between Harvard Business School professors, Spencer Stuart, and WomenCorporateDirectors Foundation, women board directors tend to look at the bigger picture of an organization and focus on long-term strategy. As such, they are more attuned to focus on long-term risks.

The report further showed that cybersecurity is one of the top three issues that directors are concerned about, and women directors show a higher level of concern of this risk, among others, than their male counterparts.

However, another report released recently by the National Association of Corporate Directors found that directors' comprehension of cyber risk is low and, further, that a very low percentage of directors and/or boards have a high level of understanding of cybersecurity risks to the organization. On top of that, 31 percent of those surveyed said they were either "dissatisfied" or "very dissatisfied" with the information they receive from management around cybersecurity.

As I have said before, it is incredibly important for the board of an organization to understand and manage the data privacy and security risks of the organization, and having someone on the board that understands the risks and can educate other board members about managing the risks is imperative.

Bottom line? Women are more attuned to cyber risks to the organization, so during the next nominating committee session, consider appointing a woman to your board to help manage those risks to the company.

— Linn Foster Freedman

UPCOMING EVENTS

Authors' Events

In addition to their legal practice and involvement with the blog, our Data Privacy + Security Team regularly serve as presenters at topic-related seminars, and participate on panels that discuss developments in the area. Several speaking engagements at scheduled events are featured below:

- May 20 – Annual Massachusetts Bar Association Health Law Conference (Linn F. Freedman & Kathryn M. Rattigan)
- June 7 – The Quorum Initiative Cyber Intrusions event in Washington D.C. (Linn F. Freedman)
- June 8 – The Quorum Initiative Cyber Intrusions event in New York City (Linn F. Freedman)
- June 22 – National Scholarship Providers Association in Rocky Hill, CT (Linn F. Freedman)
- June 23 – MCLE: Data Security 2.0: The Cloud, Mobile Devices & Encryption Webcast Panel (Kathleen M. Porter)
- July 11 & 12 – Seventeenth Annual Institute on Privacy and Data Security Law (Kathleen M. Porter)

For more thoughtful and timely discussions of legal news and perspectives on issues relating to data privacy and security, subscribe to our *Data Privacy + Security Insider* blog by e-mail or by RSS feed.

We welcome your feedback and ideas on topics you'd like us to cover. We also encourage you to share this *Insider* and the blog with anyone you think would find it useful.

If you have any questions, please reach out to your contact at Robinson+Cole or Linn F. Freedman, chair of our Data Privacy + Security Team.