Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

August 11, 2016

ENFORCEMENT + LITIGATION

FCC Exempts Schools and Utilities from TCPA for Emergencies

On August 4, 2016, the Federal Communications Commission issued a ruling applicable to schools and utilities regarding the application of the Telephone Consumer Protection Act (TCPA) to robocalls and text messages to wireless numbers in emergencies.

The FCC ruling states that schools can make robocalls and send automated texts to wireless phones without consent in emergency situations like weather closures, fires, health risks, and unexcused absences, and messages related to the school's mission, including topics such as an upcoming teachers' conference. This interpretation is surprisingly expansive, particularly coming from the FCC.

Further, the FCC stated that utility companies may do the same to inform customers of service outages or service interruptions during severe weather conditions. The FCC stated "[T]heir customers provided consent to receive these calls and texts when they gave their phone numbers to the utility company….The information is wanted and needed by consumers, and expected if the consumer gives their telephone number" to the utility company."

This ruling is specific, helpful to schools and utility companies. and provides valuable guidance on how to structure robocalls and texts to customers during an emergency without running afoul of the TCPA.

— Linn Foster Freedman

CMS Issues Warning to Nursing Homes Regarding Abuse of Residents via Social Media

On August 5, 2016, the Centers for Medicare & Medicaid Services (CMS) issued guidance to nursing homes in a letter to state survey agencies (Letter) that addresses nursing homes' obligations to protect residents. The Letter focuses on potential psychosocial harm to nursing home residents caused by the sharing on social media of demeaning photographs or recordings of residents taken by nursing home staff. The Letter appears to have been issued partly in response to a recent investigation by ProPublica, which found numerous instances of alleged abuse of nursing home residents connected to social media postings.

The Letter emphasizes in pertinent part that nursing home residents are entitled by law to:

- personal privacy and confidentiality of their personal and clinical records; and

- be free from verbal, sexual, physical, and mental abuse (which includes without limitation humiliation, harassment, threats of punishment, or deprivation).

CMS specifically cites, as an example of mental abuse, taking photographs or recordings (using cameras, smart phones, or other electronic devices) that demean or humiliate a resident and may be distributed through text messages or social media (e.g., on Twitter, Facebook, Instagram, Snapchat, or a combination of those and/or similar apps).

In the Letter, CMS reminds nursing homes of their ongoing obligation to protect residents, which includes implementing and developing written policies and procedures that prohibit all forms of abuse of residents and providing training on such policies and procedures to all staff that provide care or services to residents. Nursing homes must prohibit staff from using any equipment to take, keep, or distribute demeaning or humiliating photographs or recordings of residents. Nursing homes are also required to thoroughly investigate, respond to, and report allegations of resident abuse, and are expected to foster an environment that encourages reporting without fear of retaliation.

The Letter directs state surveyors, starting in September 2016, to request and review nursing home policies and procedures that prohibit staff from taking or using (including by texting or posting on social media) photographs, videos, or other recordings in any manner that could demean or humiliate the resident of a nursing home. Therefore, nursing homes would be well-advised in the coming weeks to review, update, and provide appropriate training to staff on resident abuse prevention policies and procedures in anticipation of heightened scrutiny from state survey agencies.

— Conor O. Duffy

Online Contacts and Eyewear Retailer Pays $100,000 Penalty to New York AG for Security Failures

Online retailer Provision Supply LLC (Provision Supply), operator of EZContactsUSA.com (which sells contacts and eye glasses), settled with the New York attorney general last week for its failure to notify its web customers of a data breach that may have exposed 25,000 credit card numbers. Provision Supply will pay a $100,000 penalty and must improve its data security practices. New York Attorney General Eric T. Schneiderman said that the breach occurred back in August 2014, but Provision Supply did not learn of it until about a year later when its merchant bank informed Provision Supply that its customers' credit cards were displaying fraudulent charges. After learning of these fraudulent charges, Provision Supply investigated the breach and hired a third party to remove the malware, but it never informed its customers or law enforcement/the Attorney General of the incident, which is in violation of the New York's Information Security Breach and Notification Act.

Additionally, the attorney general said that while Provision Supply's EZContactsUSA.com website said that it was "100 percent safe and secure," EZContactsUSA.com lacked a written security policy to address security issues, had no effective server and firewall configurations to guard against unauthorized access, and did not install antivirus or antimalware software or conduct reviews of site performance and security configuration.

Since just the beginning of this year, the New York Attorney General's Office has noticed a 40 percent increase in data breach notifications to its office.

— Kathryn M. Rattigan

Two Class Action Suits Filed against Banner Health Less Than a Week after Notices Are Sent

Regarding Data Breach

We previously reported that Banner Health (Banner) started sending notices to over 3.7 million individuals about a data breach that started with food and beverage purchases and ended up compromising employee and patient information [view related post here]. This data breach is the largest so far this year.

Less than a week after Banner started sending out the notices to individuals, two class action lawsuits have been filed against it—one by a physician and one by a physician assistant.

Just days following the notification, a physician on staff at Banner filed a class action lawsuit against Banner alleging that Banner was negligent and allowed the breach to occur. He seeks identity protection and credit monitoring despite the fact that Banner is offering free credit and identity monitoring for one year.

According to the plaintiff, this is a "skimpy fix," and the plaintiffs in that suit will be "asking for a more robust package."

The second suit, filed in Arizona on August 9, 2016, by a physician's assistant employed by Banner, alleges that Banner neglected its duty to protect sensitive information. It states that "[T]his data breach is a direct result of Banner Health's failure to implement adequate cybersecurity measures commensurate with the duties it undertook by storing large amounts of customer information on its computer servers."

The suit further alleges that one year of credit and identity monitoring for one year is "inadequate," and Banner's provision of details surrounding the breach is "alarming." The suit contends that Banner has not provided sufficient information to the affected individuals about the breach. The suit seeks compensatory and punitive damages.

— Linn Foster Freedman

DATA BREACH

Oracle's MICROS Point of Sale Division Hacked

KrebsonSecurity has reported that the Russian organized cybercrime group, dubbed the Carbanak Gang, which in the past has been suspected of stealing more than $1 billion from banks, retailers, and hotels, and restaurants worldwide, may have breached "hundreds of computer systems" at Oracle Corp's MICROS division.

It is further reported that Oracle's MICROS division is one of the top three point-of-sale vendors globally, and the compromise includes a customer support portal for the point-of-sale systems used by companies throughout the world, including approximately 330,000 sales registers worldwide.

Oracle has confirmed that it has detected malicious code on some of the MICROS systems and is asking customers to reset their passwords for the MICROS online support portal. This writer has received several emails already from multiple well-known hotel chains used for travel stating my password has automatically been reset. Word to the wise: reset your passwords frequently.

— Linn Foster Freedman

HIPAA

Record HIPAA Settlement Paid by Hospital Chain

Federal regulators announced last week that Illinois' largest hospital chain would pay $5.5 million, a record payment under the Health Insurance Portability and Accountability Act (HIPAA), in connection with three 2013 data breaches that affected the protected health information of millions of its patients. The Advocate Health Care Network, which manages 12 hospitals and hundreds of satellite offices, agreed to the settlement after the Office of Civil Rights at the U.S. Department of Health and Human Services determined that Advocate did not properly limit access to electronic systems nor adequately assess risks of its electronically held PHI.

The breaches resulted from three separate incidents: (1) the theft of four laptop computers from an office building, (2) unauthorized access into a business associate's computer network, and (3) the theft of an unencrypted computer from an employee's unlocked vehicle. Approximately four million individuals were affected.

In addition to the monetary payment, Advocate agreed to a number of security improvements, including a risk analysis for ePHI, adopting a plan for managing security risks, and expanded HIPAA training. In a statement released after reports of the settlement, Advocate noted that there has been no indication that any of the acquired PHI was misused.

The settlement is further evidence of the OCR's efforts to ramp up audits to gauge HIPAA compliance and enforce violations where they exist. To date, 2016 HIPAA settlements total $20.4 million, which already far exceeds the annual record of $7.9 million in 2014. In light of OCR's enforcement efforts, health plans, providers, and other covered entities may want to be vigilant in their HIPAA compliance by, among other things, engaging in a comprehensive risk analysis and risk management to ensure that individuals' PHI is secure.

— Brian J. Wheelin

CYBERSECURITY

White House Directive Outlines Who to Call for Help with a Cyber Incident

Last week, the White House issued a new directive that outlines how the government handles significant cyber incidents, which gives the public information on which agency to call in the event of a cyber incident. We often get asked, "Whom do we call—the FBI, the Secret Service, the DOJ, etc.?"

The directive outlines what incidents are considered to be significant. The definition of a significant incident is one that will likely result in at least a demonstrable impact to public safety, national security, economic security, foreign relations, civil liberties, or public confidence. You can access the directive here.

— Linn Foster Freedman

Researchers Say Chip-Based Credit Cards Aren't as Secure as We Thought

Payment technology company NCR Corporation (NCR) determined last week that the new chip-based

credit card technology isn't as secure as we thought. The technology behind these chip cards that is supposed to make them more secure than the obsolete magnetic strip cards is that, if an individual uses the magnetic strip and the card also has a secure chip, the magnetic strip will tell the payment machine to reject that method of payment and instruct the individual to insert the card into the machine for chip processing. However, NCR discovered that credit card thieves can rewrite the magnetic strip code so that it appears like a chipless card and will allow the thieves to keep counterfeiting the cards. NCR says that the problem is that, while retailers are encouraging the use of chip cards, they are upgrading their payment machines but are notencrypting the transaction. Retailers would need to pay extra for the encryption. So, while they are spending money on the new payment machines for chip cards, the transaction is still not all that secure. NCR researches advise retailers to encrypt everything in a transaction to avoid large-scale data breaches like those at Target and Home Depot.

— Kathryn M. Rattigan

LastPass Security Vulnerabilities Discovered

Passwords have always been a challenge. It is hard to remember them, and you are not supposed to use the same password across different platforms. Several companies, including LastPass, have tried to help consumers with managing passwords in a secure way so they can keep them straight. Unfortunately, last week two security researchers reported that they had discovered several security vulnerabilities.

The first vulnerability allowed the execution of code remotely and was reportedly fixed last week. The second vulnerability was discovered and patched over a year ago but could have been exploited to steal stored credentials. The vulnerability was described as a "complete remote compromise."

Users of LastPass may wish to consider changing their passwords that were stored in a LastPass account.

— Linn Foster Freedman

DRONES

Many Big Announcements for the UAS Industry and Its Safety and Privacy Initiatives

The commercial drone industry is projected to generate over $82 billion for the U.S. economy and over 100,000 new jobs by 2025. Last week, at the White House Office of Science and Technology Policy's (OSTP) "Workshop on Drones and the Future of Aviation," it was announced that several key players (both in the private and government sectors) will launch an accelerated initiative to integrate unmanned aircraft systems (UAS) into the U.S. airspace. Here is a quick summary of those initiatives:

- The National Science Foundation will contribute $35 million in research funding related to intelligent and effective UAS design, control, and application over the next five years.
- The U.S. Department of the Interior will use UAS for search and rescue operations, to augment manned aircraft operations, to improve government processes around technological adoption, and to increase data sharing of wild fire locations.
- There is a collective commitment by UAS industry associations to implement broad educational efforts around privacy best practices.
- The Federal Aviation Administration (FAA) plans to publish proposed rule for "Operations of Small UAS over People" this winter.
- The FAA will collaborate with UAS industry stakeholders to charter an Unmanned Aircraft

System Team to use a data-driven, consensus-based approach to analyze UAS safety.

- The National Oceanic and Atmospheric Administration will use UAS for precise gravity measurements and augmenting observation capabilities from ships.
- The U.S. Postal Service's Office of Inspector General intends to publish findings and analysis on the public's evolving opinion of drone delivery as a potential future means of logistics technology.
- New York State's Empire State Development will commit $5 million to strengthen the state's efforts to create a hub for UAS innovation and manufacturing.
- The Northern Plains UAS Test Site in North Dakota plans to start conducting beyond visual line of sight flights that will start on the earth's surface and reach heights of about 29,000 feet.
- Zipline International, Ellumen ASD Healthcare, and Bloodworks Northwest plan to use UAS technology to disseminate critical care supplies to remote areas of the U.S.
- Flirtey and International Medical Corps plan to focus their efforts on humanitarian applications of UAS technologies.
- Women of Commercial Drones and the Commercial Drone Alliance are creating a program to advance women's participation in the UAS industry.
- DroneBase and Drones & Good will start a program for providing transitioning military veterans with UAS training programs and apprenticeships in the commercial drone industry.
- Future of Privacy Forum and PrecisionHawk released the report "Drones and Privacy by Design: Embedding Privacy Enhancing Technology in Unmanned Aircraft." The report highlights technologies and practices that can help drone operators and commercial drone manufacturers minimize data collection and retention, obfuscate individuals' images, and better secure the data (especially the personally identifiable data) they collect using UAS technologies.

This is surely an exciting time for commercial drone operators and manufacturers alike. The industry will continue to enhance its technologies and safety features, hopefully with an eye for privacy in the skies.

— Kathryn M. Rattigan

VIRTUAL CURRENCY

Bitcoin Exchange Bitfinex Hacked

Bitcoin Exchange Bitfinex, based in Hong Kong, was hacked last week, incurring a whopping loss of $65 million. It was shut down last week after 119,756 bitcoins were stolen from users' accounts.

According to Bitfinex, "after much thought, analysis and consultations" it has decided to spread the loss across all of its users, including those who were not affected by the hacking incident. That means a loss of about 36 percent of each user's account.

Bitfinex will replace that part of a user's account with a BFX token, and the company will keep track of the token and attempt to replace the amount lost in the future.

Although the exchange was back up today, trading, deposits, and withdrawals remain suspended.

— Linn Foster Freedman

PRIVACY TIP #47

Safety Tips for Using Twitter When Anonymity Is Crucial to Your Safety

My Facebook account got hacked, so I am no longer on Facebook. LinkedIn was also hacked and users were told to reset their passwords, which I did immediately. I don't use Twitter because it's just another way to get hacked, and those of you who know me know I am too paranoid about my data privacy to get too far out there on social media.

But that's me—a paranoid data privacy and security professional that some have jokingly said should go hide under a rock.

People love Twitter and tweet, tweet, tweet about everything. But what about individuals who are or have been the victim of domestic violence, and anonymity is crucial to their personal safety? How can they use Twitter to have fun but do it in a way that is safe?

The National Network to End Domestic Violence, with the support of Twitter, recently released a must-read guide called "Safety & Privacy on Twitter: A Guide for Survivors of Harassment and Abuse."

The guide provides safety tips for users to help them make informed choices about their user name, password, notification settings, using different photos for different sites to keep them from being linked, maintaining location privacy, how to limit access to only followers, and how to have a private conversation on Twitter, all of which are designed to assist Twitter users to control and protect their privacy. It supports victims' ability to use social media and have fun but provides tools that will help victims control their privacy, and therefore, use Twitter in a safe way.

Kudos to both companies for providing these tips for victims of domestic violence. The guide can be accessed here.

— Linn Foster Freedman

UPCOMING EVENTS

Authors' Events

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

- September 12 - 15 – (ISC)² Security Congress in Orlando, FL (Linn F. Freedman)
- October 11 & 12 – InfoGovCon in Providence, RI (Linn F. Freedman)
- October 24 - 26 – Privacy + Security Forum in Washington, D.C. (Linn F. Freedman)
- November 15 – ABA Webinar: "Assessing the Situation: How to Identify and Evaluate the Cyber and Data Risks that a Contractor Bears" (Linn F. Freedman)

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.

Boston | Hartford | New York | Providence | Stamford | Albany | Los Angeles | Miami | New London | rc.com

Robinson & Cole LLP