Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

February 11, 2016

CYBERSECURITY

President Obama Establishes Commission on Enhancing National Cybersecurity

Yesterday, President Obama, by Executive Order, established the Commission on Enhancing National Cybersecurity within the Department of Commerce.

The Commission will comprise up to 12 members, including "those with knowledge about or experience in cybersecurity, the digital economy, national security and law enforcement, corporate governance, risk management, information technology (IT), privacy, identity management, Internet governance and standards, government administration, digital and social media, communications, or any other area determined by the President to be of value to the Commission."

The mission of the Commission will be to make recommendations "to strengthen cybersecurity in both the public and private sectors while protecting privacy, ensuring public safety and economic and national security, fostering discovery and development of new technical solutions"…and developing public-private partnerships and relationships around best practices around cybersecurity, including appropriate technology.

The Commission will provide recommendations for upgrading the federal civilian IT systems and infrastructure, enhancements to protect critical infrastructure, and assistance for state and local governments to enhance cybersecurity.

The Commission is to provide a final report by December 1, 2016, which will be published on a public website thereafter, and the Commission will terminate 15 days after it issues its final report, unless extended by the President.

It is unclear what will happen to the recommendations thereafter, which is disappointing. As we know in the data privacy and security world, cybersecurity is a never-ending process that must be continually assessed, refined and updated. Hopefully, there will be a continued effort by the government after the Commission's work, report, and recommendations.

— Linn Foster Freedman

FDIC Cybersecurity Framework Features Four Areas Critical to Bank Security

Long gone are the days when a financial institution's primary security concern was protecting cash in the

bank vault, the Federal Deposit Insurance Corporation (FDIC) acknowledges in its recent article, "A Framework for Cybersecurity," released February 1, 2016. Instead, the framework asserts that cyber-attacks now represent "one of the most critical challenges facing the financial services sector," and highlights four information security components essential to combatting the most common types of cyber-attacks:

1. Corporate Governance of Cybersecurity. To effectively combat electronic threats, financial institutions must foster a corporate culture prioritizing cybersecurity. Bank management and the board of directors bear the responsibility of establishing cybersecurity as an "enterprise-wide initiative" spanning all divisions of the financial institution.

2. Threat Intelligence. The FDIC framework provides a number of resources that are available to help financial institutions gather, analyze, understand, and share information about digital vulnerabilities and threats. The Financial Services Information Sharing and Analysis Center (FS-ISAC) is an information-sharing forum that includes analysis and mitigation strategies relating to information security, disaster recovery, fraud investigations, and payment system risk. The Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT) focuses on current security issues and provides alerts as well as publications, educational material, and assistance with cyber threats.

3. Security Awareness Training. A financial institution's risk control structure is only as secure as its most careless employee, making cybersecurity awareness training vital to preventing cyber-attacks. Mandatory security training encouraging employees and contractors to adopt the maxim "Think Before You Click" should be implemented company-wide, with role-specific trainings tailored to individual departments.

4. Patch-Management Programs. Regular software updates (patches) addressing known security weakness and vulnerabilities in computer applications and operating systems can significantly reduce the number of security incidents faced by a financial institution. The FDIC suggests that an "effective patch-management program should include written policies and procedures to identify, prioritize, test, and apply patches in a timely manner."

The FDIC framework includes additional resources for financial institutions wishing to improve cybersecurity and is available online here.

— Norman H. Roos and Scott M. Baird

ENFORCEMENT + LITIGATION

Lincare, Inc. Ordered to Pay Civil Monetary Fines for HIPAA Violations

In an unusual scenario, in fact only the second time in history, the Office for Civil Rights (OCR) was successful before an Administrative Law Judge (ALJ) in obtaining an order for the payment of civil monetary fines as a result of HIPAA violations.

The OCR assessed a penalty of $240,000 against Lincare Holdings, Inc. (Lincare) for failing to safeguard the PHI of 270 patients. Lincare appealed the assessment to an ALJ The case stemmed from a complaint of the ex-husband of an employee of Lincare, who reported to Lincare and the OCR that his ex-wife left PHI of patients of Lincare in a car that she left with him. He was not authorized to access or view the PHI.

At the time, employees were allowed to take PHI from the premises and were ordered to keep copies of documents in their car in the event that something happened to the building. The judge stated that the company had no policies or procedures to monitor or provide for the security of the documents. She

further held that Lincare failed to take reasonable steps to protect the PHI.

Following the decision, the OCR stated, "…all covered entities, including home health providers, must ensure that, if their workforce members take protected health information offsite, they have adequate policies and procedures that provide for the reasonable and appropriate safeguarding of that PHI, whether in paper or electronic form."

This is another example of PHI being left in a car and either lost or stolen, with devastating consequences. Companies that allow employees to take PHI offsite may wish to review and implement travel policies and encryption technology for removable media.

— Linn Foster Freedman

FTC Settles Case against Vulcun for Installing Apps on Users' Phones without Permission

On February 5, 2016, the Federal Trade Commission (FTC) announced that it has agreed to settle its case against Vulcun, alleging that it "unfairly replaced a popular web browser game with a program that installed applications on consumers' mobile devices without their permission."

Vulcun purchased the game Running Fred, which is used by over 200,000 users, and replaced it with Vulcun's extension application directly onto Android devices and bypassed the Android operating system permission process.

According to the FTC, "After Vulcun acquired the Running Fred game, they used it to install a different app, commandeer people's computers, and bombard them with ads." After doing so, numerous consumers complained to Google, the owner of Google Chrome and Android, stating that apps were being installed on their devices without their permission and would reinstall after being deleted.

The settlement includes the requirement that Vulcun tell consumers about the types of information accessible through a product or service, how it will be used, how to display permissions notices, and how to get consumers' affirmative consent before installing or materially changing a product or service. It also requires it to delete all information from consumers that it collected prior to the date of the order within 10 days. As with most settlements, the order will be in effect for the next 20 years. The agreement with Vulcun is available for public comment through March 8, 2016, and then will be voted on by the commission.

— Linn Foster Freedman

TCPA Class Action against Sabre (Hawaiian Airlines) Tossed Out

Last week, the Ninth Circuit dismissed a Telephone Consumer Protection Act (TCPA) class action against Sabre Inc. (Sabre) because the court determined that the lead plaintiff, Shaya Baird, had consented to receiving text messages by providing her phone number when she booked a flight with Hawaiian Airlines. Baird's complaint alleged that Sabre sent her an unsolicited text message regarding flight notification services. Baird did not respond to that text message, and she did not receive any further text messages. Baird argued that she had no choice but to provide her phone number when she booked the flight, and she was not given any opportunity to opt out of receiving text messages.

The court said in its decision, "Baird knowingly released her phone number to Hawaiian Airlines while making a flight reservation. She did not provide any "'instructions to the contrary' indicating that she did

not ‘wish to be reached’ at that number.” Moral of the story: if you provide your phone number to your airline, expect a text message or two.

— Kathryn M. Rattigan

Shutterfly Requests Reconsideration of Denial of Motion to Dismiss in Biometrics Case

We previously reported that Shutterfly Inc. was unsuccessful in persuading an Illinois federal judge to dismiss the biometrics case against it (view related posts, here and here).

Last week, Shutterfly moved for reconsideration of the denial, basing the request in part on Facebook’s success in convincing another Illinois judge to dismiss a similar case against it alleging violation of the Illinois Biometric Information Privacy Act (view related post).

Shutterfly requested that, if the judge does not grant its request for reconsideration, the judge certify the case so it can take an interlocutory appeal before the case is finally decided.

We will continue to watch biometric cases closely as they wind their way through the court system.

— Linn Foster Freedman

HEALTH INFORMATION

HHS Proposes Updates to Confidentiality of Part 2 Substance Abuse Treatment Records

On February 5, 2016, the Department of Health and Human Services (HHS) issued proposed changes to the Confidentiality of Alcohol and Drug Abuse Patient Records regulations, also known as “Part 2 records,” which were published in the Federal Register on February 9, 2016.

The proposed changes update Part 2, which was originally enacted in 1975, to take into consideration the way health information is exchanged today—electronically—and within new models of delivering health care to patients.

The changes in the proposed rule include:

- allowing Part 2 data to be included in scientific research studies with specific requirements to protect confidentiality
- revising the definition of what falls within a Part 2 program so that Part 2 rules do not apply to general medical facilities or general medical practices but only to specialized substance abuse treatment programs
- allowing a patient to provide a more generalized authorization for the release of substance abuse treatment information as long as the patient gets a list of those providers who may have access to the information “to support increased participation of individuals with substance use disorders in integrated care by allowing more flexibility for information sharing and including additional confidentiality protections"
- including the protections to both paper and electronic records

As someone intimately involved in the Substance Abuse and Mental Health Services

Administration's (SAMHSA) undertaking over the past few years to understand and address concerns about individuals being treated for substance use having access to and receiving integrated care from providers, I feel this is great news and applaud SAMHSA.

The proposed changes are open for public comment until 5:00 p.m. on April 11, 2016. To submit comments electronically, go to http://www.regulations.gov.

— Linn Foster Freedman

DRONES

Connecticut Audubon Society Joins the No Drone Zone List

Drones are no longer permitted at 19 of the Connecticut Audubon Society's (CAS) sanctuaries because of the annoyance to visitors and harassment of wildlife. This is one of the first sanctuaries in the country, and certainly the first in Connecticut, to establish a "no-drone" policy. To date, there has only been a couple drone-related incidents in a CAS sanctuary, but the organization is saying they are instituting the ban proactively due to the increase of drones hitting our skies since the holidays. CAS President Alexander Brash said, "No creature–great or small, human or wildlife–visits our sanctuaries hoping to be buzzed by a drone. We are taking this action to protect the birds and animals that consider our sanctuaries home, and to ensure that our sanctuaries are also a place of respite for our human guests too." We may see other organizations like the CAS follow suit.

— Kathryn M. Rattigan

INTERNET OF THINGS

Are Kids' Connected Toys Secure Enough?

If the Hello Barbie complaints weren't enough, now it has been announced that researchers determined that the kids' toys the Fisher-Price Smart Toy Bear and the hereO GPS watch had some serious security vulnerabilities. The Smart Toy Bear's backend programming used unsecured application programming interfaces (APIs) to allow portions of software code to interact. Sounds technologically okay, but because these APIs were unsecured, it allowed hackers to access information about registered children, such as name, dates of birth, gender, and spoken languages. Mattel has since addressed these issues in the Smart Toy Bear.

The hereO GPS watch used the same type of APIs and allowed hackers to access family members' locations, GPS logs, and even other features of the kids' watch, such as spying on communications. Again, hereO GPS watch manufacturer fixed these bugs and dealt with these issues.

While both toys' security vulnerabilities were patched, the larger concern is how we can better protect children's privacy moving forward. With more and more connectivity being available for younger children, perhaps we need better guidelines for toy manufacturers when it comes to privacy and security.

— Kathryn M. Rattigan

DATA PRIVACY

Biometrics Institute Issues New Privacy Guidelines

The Biometrics Institute issued new privacy guidelines for collecting and safeguarding biometric data, such as fingerprints and iris scans. The guidelines contain 16 principles that should be considered when collecting and using biometric data, including proportionality, informed consent, protection of the data, purpose, retention and the importance of privacy impact assessments.

Chief Executive Isabelle Moeller of the Biometrics Institute, said, "The Biometrics Privacy Guidelines have been designed by the Biometrics Institute to provide a guide for suppliers, end users, researchers, managers and purchasers of biometric systems. It is the public's assurance that the biometric managers have followed best practice privacy principles when designing, implementing and managing biometric based projects." These guidelines will be distributed to more than 190 member organizations in 24 countries.

— Kathryn M. Rattigan

PRIVACY TIP #21

It's a New Year—Time to Get a Free Copy of Your Credit Report

I am fortunate to teach the Privacy Law class at Roger Williams University School of Law on Tuesday afternoons. Today, we discussed all of the laws relating to the financial services industry. Okay, although not the most exciting content, the discussion included the Fair and Accurate Credit Transaction Act (FACTA). Enacted in 2008, FACTA allows individuals to obtain a free copy of their credit report every 12 months from each of the three credit reporting agencies—Experian, Equifax and TransUnion. In class today, we discussed why it is important for consumers to be able to obtain a copy of their credit report and why it is important to make sure it is accurate. We also decided that each of us should get a copy of our credit report.

Here is what we concluded. There are a number of entities that have obtained a credit report on each of us. The types of entities that can request a credit report include financial services companies that will give you credit if you are buying a car or a house; a credit card company if you are applying for a credit card; utilities that provide services to you; entities that provide a professional license; insurance companies; or your prospective employer. All of the entities that have requested information about your credit will be included on your credit report. It is important to understand who has requested and obtained information about you and your credit and what they were told by the credit reporting agencies.

If anyone has tried to open an account in your name without your knowledge, this will be included on your credit report as well. It is an indication of whether you are or may become the victim of identity theft. If you were notified of any of the massive data breaches this year, and your Social Security numbers were compromised, this is a real risk. Getting a copy of your credit report will let you know if anyone has tried to open an account in your name and whether it was opened.

Plus, it's free! It is important information for your financial well-being, particularly if you are about to purchase a home or car, or start a new job. How do you get it? Go to www.annualcreditreport.com. This is the only authorized website to obtain your credit report. Or call 1-877-322-8228. You will have to provide your personal information to authenticate your identity.

Once you get your report, check it carefully, and if there are any discrepancies or errors, you can call the credit reporting agency that issued the report and notify it that it is not accurate as well as the company that provided the inaccurate information. You can also contact the FTC for assistance at www.ftc.gov.

I don’t know about you, but I am signing off so I can go get my credit report right now…

— Linn Foster 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.