April 21, 2016

UPCOMING EVENT

Recent Trends in Cyber Intrusions — A View from the Insiders

Although sharing information may alleviate companies from "going it alone" and can give them the heads up about intrusions so they can adequately prepare and respond, private companies are understandably nervous about giving cyber intrusion information to the government and exposing vulnerabilities. Can they trust the government to keep business information strictly confidential? How does the government protect the information?

Join us on Tuesday, May 3, 2016, at Brown University in Providence, Rhode Island, for this panel discussion with Peter F. Neronha, U.S. Attorney for the District of Rhode Island; David C. Aaron, Trial Attorney, U.S. Department of Justice National Security Division, Counterintelligence & Export Control Section; Linn F. Freedman, Chair of Robinson+Cole's Data Privacy + Security Team; a FBI Cybercrimes Agent; and a Secret Service Agent.

Registration begins at 7:30 a.m. and the program runs from 8 to 10 a.m. Continental breakfast will be provided.

For more information and to register, click here.

Co-hosted by Brown University Executive Master in Cybersecurity and Robinson+Cole. Robinson+Cole and Brown University are not affiliated.

ENFORCEMENT + LITIGATION

Shutterfly Settles Illinois Biometrics Case

We previously reported that Shutterfly's effort to dismiss the proposed biometrics class action case against it was unsuccessful.

The proposed class action suit alleged that Shutterfly violated the Illinois Biometric Information Privacy Act because Shutterfly measured the contours of the named plaintiff's face to create a template that it used to suggest that other photos of him be tagged with his name, also known as a "faceprint." The judge was unwilling to dismiss the case at its earliest stage.

Last week, the case was settled and both parties moved to dismiss the case. The details of the settlement have not been released.

Facebook still battles a similar case in Illinois for collecting facial data through its facial recognition program. It states it will "vigorously defend" the suit. Facebook has been offering its tagging program since it acquired Face.com in 2012. Facebook reportedly holds the largest amount of biometric face recognition data in the world.

— Linn Foster Freedman

Robocalls Offering 'Free Cruise' for Completion of Political Survey TCPA Violation

This week an Illinois court found that Economic Strategy Group (ESG) violated the Telephone Consumer Protection Act (TCPA) by making robocalls to almost 1 million individuals purporting to be conducting a political survey but also offering a "free cruise" for taking part in the survey. U.S. District Judge Matthew F. Kennelly said in his lengthy order, "The evidence is uncontroverted that a prerecorded message was played on each call"; "this is a violation of the TCPA, irrespective of whether the calls were made by or on behalf of a tax-exempt non-profit, were made for a political or non-commercial purpose, or did not make reference to or play long enough to mention defendants' vacation products." However, the court did not determine whether the robocalls were made on ESG's own behalf or on behalf of Caribbean Cruise Line, Inc., Vacation Ownership Marketing Tours Inc., and the Berkley Group Inc. The judge said he will leave it up to a jury to decide the direct or indirect liability of each defendant in this case.

— Kathryn M. Rattigan

DATA BREACH

Ashley Madison Attorney-Client Communications Leaked in Data Breach

We all remember the Ashley Madison data breach [view related posts here and here]. The hackers, calling themselves "The Impact Team," requested that the Ashley Madison extramarital affair site and Cougar Life and Established Men sites be "taken down." When they weren't, they posted details (9.7 gigabites worth) to the dark web of approximately 37 million users.

Of course, lawsuits were filed (we are not counting, but reportedly "hundreds") by anonymous plaintiffs. The judge ruled that the named plaintiffs had to identify themselves if they wanted to represent the class.

In a recent twist, the plaintiffs' lawyers have informed the court that emails between the owner of Ashley Madison and its lawyers were part of the information that was posted online and subsequently viewed by members of the media. Following media reports that there are emails between the company and their lawyers that mention "methods of hiding the fake female profiles from Ashley Madison members," the plaintiffs' attorneys have petitioned the court to use those emails to help prove that Ashley Madison defrauded its members.

Usually, emails between an attorney and client are protected by the attorney-client privilege. In this case, since the emails were leaked and posted online, they were available to the public. The plaintiffs are trying to use the crime-fraud exception to the attorney-client privilege to allow use of the documents in the litigation. Ashley Madison says "stolen documents do not lose their privileged status because they are published without the consent of the privilege holder."

We will be watching this issue closely as it appears to be a case of first impression of whether a litigant can use hacked documents to support claims against the hacked company.

— Linn Foster Freedman

CYBERSECURITY

New Report Warns Health Care Industry to Expect More Ransomware Attacks

A new report of a survey of around 30 midsized hospitals by the Health Information Trust Alliance (HITRUST) concludes that health care entities should be prepared for an increase in ransomware attacks in the near future.

HITRUST surveyed the hospitals in late 2015 and found that 52 percent of the hospitals were infected with malicious software, including ransomware.

Four hospitals have already recently fallen victim to ransomware—Hollywood Presbyterian, Ottawa Hospital, MedStar, and Methodist Hospital—causing significant disruption to patient care.

This report's conclusions verify what we all have been predicting: hackers will continue to use any means available to make a quick buck and the health care industry is an easy target. Health care entities may wish to consider preparing for a ransomware attack now, including testing their backup system and contingency operation planning and implementation.

— Linn Foster Freedman

DATA PRIVACY

Biometric Fingerprinting Technology to Expand

Using our fingerprints to unlock our smartphones is pretty commonplace at this point. Sweden's Fingerprint Cards (FPC), a business specializing in biometrics, says that fingerprint identification will become the fastest-growing market by 2018. After Apple introduced its iPhone fingerprint sensors, FPC's market value increased to around $4.1 billion (a surge of about 1,600 percent for FPC).

But FPC is thinking much bigger than just iPhones; FPC says that biometric fingerprinting can be used for allowing access to buildings and IT systems as well as for keyless entry to your car. FPC predicts that the biometrics business could expand to roughly 100 million sensors in 2017 and around 500 million by 2018.

Many biometrics supporters argue that this fingerprint technology offers better security and simplicity when compared to using pin codes for identification. Watch for biometric fingerprinting to continue trending upwards.

— Kathryn M. Rattigan

HIPAA

OCR Issues Audit Protocol and Targets Over 800 Entities—Business Associates Too

The Office for Civil Rights (OCR) has issued its revamped audit protocol for its second phase of auditing covered entities and business associates' compliance with the HIPAA Privacy, Security and Breach Notification Rules.

The lengthy audit protocol is posted on the OCR website. It provides general instructions and then cites each statutory section of the Privacy, Security and Breach Notification Rules that will be covered by the audit. For instance, pursuant to 45 C.F.R. Section 164.510(b), the OCR will look at "What policies and procedures exist for disclosing PHI to family members, relatives, close personal friends, or other persons identified by the individual?" and will "Obtain and review policies and procedures for such disclosures."

An example of a question related to compliance with the Security Rule is 45 C.F.R. Section 164.308(a)(5)(i): "Does the entity have policies and procedures in place regarding a security awareness and training program? Does the entity provide security awareness and training to all new and existing members of its workforce? Obtain and review policies and procedures for security awareness and training program." The documents the OCR mention include obtaining the training materials to determine if they are "reasonable and appropriate for workforce members to carry out their functions" and "Obtain and review documentation demonstrating that the security awareness and training programs are provided to the entire organization and made available to independent

contractors and business associates, if appropriate."

In the section outlining the review of breach notification compliance, the OCR indicates that if a covered entity or business associate determined that an acquisition, access, use, or disclosure of PHI did not require notification, "did the covered entity or business associate determine that one of the regulatory exceptions...apply? If yes, obtain documentation of such determination."

The OCR has been warning covered entities and business associates about the new phase of audits for over a year. Now that we have the protocol, it can be used as a roadmap for preparing for an audit or getting compliance in order.

We are hearing through the grapevine that over 800 covered entities and business associates will get the "letter" from the OCR to start the audit process. If you get the letter (which the OCR says you will not get if there is a pending investigation), get ready. If you don't get the letter in this wave, still get ready. Use the roadmap as guidance that we rarely get from the OCR.

— Linn Foster Freedman

HEALTH INFORMATION

OIG Laments Failure to Comprehensively Address EHR Fraud

The U.S. Department of Health & Human Services (HHS) Office of Inspector General (OIG) recently released a compendium (Compendium) of its top unimplemented recommendations. The Compendium comprises 25 unimplemented past OIG recommendations that the OIG believes could have a positive impact on HHS programs in terms of cost savings and/or quality improvements. The Compendium's recommendations span the breadth of HHS programs, including Medicare, Medicaid, Affordable Care Act marketplaces, and health information technology.

In December 2013, the OIG reported that hospitals had not implemented all recommended electronic health record (EHR) technology fraud safeguards in connection with the Centers for Medicare & Medicaid Services (CMS) meaningful use program. The OIG then recommended that the Office of the National Coordinator for Health Information Technology (ONC) and CMS strengthen collaborative efforts to comprehensively address fraud vulnerabilities in EHR systems subsidized through the meaningful use program. The OIG cited the improper use of the copy-paste feature in EHR systems and the failure on the part of approximately 75 percent of hospitals to incorporate policies governing the use of copy-paste in EHR systems as a particular area where EHR systems are susceptible to fraud.

The Compendium follows up on the OIG's 2013 findings to report that CMS and ONC have yet to develop a comprehensive plan to collaboratively address fraud vulnerabilities in EHR systems, although CMS has undertaken certain efforts to monitor fraud through payment audits, and the ONC has offered technical assistance to federal agencies. The Compendium notes that full implementation of its recommendations regarding EHR fraud could improve HHS program integrity and also protect personal identifying information of HHS program beneficiaries. The Compendium also posits that all divisions within HHS have a shared responsibility for the integrity of HHS programs.

Hospitals and other health care providers would do well to recognize that the OIG remains highly cognizant of the susceptibility of new health care technology to fraud, particularly as the adoption of such technology has become pervasive throughout the health care system (due in part to subsidies under programs such as CMS's meaningful use program). The Compendium provides a reminder that the OIG continues to monitor program compliance related to EHR technology, and hospitals and other health care providers would be well advised to review applicable HHS program requirements and guidance to ensure compliance with such requirements and allow for implementation of best practices for the adoption of EHR technology.

— Connor O. Duffy

DRONES

Police Department Drones Vulnerable to Hackers?

While there has been much debate over police department drones and individual privacy, now, a new concern has emerged: the threat of hackers. Recently, a security researcher, Nils Rodday, used a laptop and $40 worth of equipment to hack into a drone worth approximately $30,000. The drone Rodday specifically targeted was a police department drone, which he intercepted using its Wi-Fi connection and sending it new commands. In addition to Rodday's drone-hacking experiment, the University of Texas has also conducted hacking tests; as early as 2012, engineering professor Todd Humphreys demonstrated that drone GPS signals can be "spoofed," which allows hackers to remotely take them over.

While it might seem like police departments could spend enough on a drone in order to equip it with proper security protections from hackers, most police departments are buying drones that aren't nearly as secure as the drones operated by the U.S. military. And for most police departments and government agencies, in-house drone security experts are hard to retain (or pay). If police departments contract this work out, finding bugs and security holes may be difficult because the hacker community may not want to share their findings with law enforcement. One suggestion has been to create a program similar to "Hack the Pentagon," where police departments will pay bounties to hackers who find vulnerabilities in the systems. However, one central command center may be a better, more cost-effective approach for police departments. And at the very least, police departments and other governmental agencies utilizing drones should be using encrypted communications to increase security at the base. Keep this in mind if you are considering using drones to capture data that may be confidential or proprietary.

— Kathryn M. Rattigan

Texas Resident Makes Claims That Texas Drone Law Is Unconstitutional

Last week, Texas resident Manuel Flores filed suit in Texas challenging the constitutionality of the state's drone surveillance law. His suit claims that the law treats approximately one million residents categorically differently from those in the rest of the state. The Texas drone law at issue here, Section 423.002(a)(14) of the Texas Government Code, states that it is lawful to use drones to take photos for academic research, law enforcement and other public safety measures, mapping, and the protection of oil pipelines as well as images of real property or a person on real property within 25 miles of the U.S. border. Flores argues that this law singles out residents along the Texas-Mexico border, reduces privacy rights, and serves no legitimate law enforcement purpose because other provisions of Texas state law already allow the government to take photos or video footage of Texans anywhere in the state. Flores also argues that the law cannot survive the strict scrutiny test applied in constitutional cases because it targets a suspect category of people—those of Mexican ancestry. We will keep our eyes on this case and see how it pans out.

— Kathryn M. Rattigan

INFORMATION GOVERNANCE

Data Security Is Top Driver for Information Governance

A recent Advice from Counsel study sponsored by FTI Technology, entitled "The State of Information Governance in Corporations," found data security to be the top driver for information governance initiatives. The purpose of the study was to better understand the health and success of information governance programs within corporations. The respondents included approximately 25 in-house lawyers who were interviewed from Fortune 1000 corporations and have responsibilities that focus on e-discovery and information governance.

The respondents broke data security down into four key areas:

1. Securing sensitive personally identifiable information for clients, patients, and employees. Across all industries, respondents acknowledged a sense of responsibility for protecting the sensitive information of their customers and employees.
2. Securing sensitive company intellectual property.
3. Creating a tiered security network to protect against data breaches.
4. Developing protocols and systems to ensure secure access to the network for partners and other approved third-party providers.

Categorizing data security into these four buckets can help companies prioritize internal projects and continue to make forward progress. The key is to break down large projects into smaller and more manageable ones that are easier to accomplish.

Some projects companies could consider this year include the following:

- identifying where sensitive company intellectual property is stored
- conducting an inventory of data repositories and documenting access permission levels
- protecting customers' sensitive data, including credit card information, social security numbers, etc.
- ensuring third-party providers sign a nondisclosure agreement (NDA) if it's known they will have access to sensitive company data, in particular customer data

It's true that some of these projects may require the purchase of new technology, engagement of other counsel, and comprehensive training. However, it's certainly well worth the effort.

— *James A. Merrifield*

PRIVACY TIP #31

Landlines Still a Safe Way to Communicate but Telephone Companies Want to Drop Them

I am pretty up-to-date on data privacy and security and technology, but the *60 Minutes* episode this past Sunday night floored even me. If you didn't see it, it is worth streaming.

Basically, *60 Minutes* showed Karsten Nohl, a German computer scientist, remotely attacking U.S. Congressman Ted Lieu's cell phone and listening to his cell phone calls. I mean, listening to every conversation clear as day. The spying was allowed by security bugs in the global telecommunications network known as Signaling System No. 7 (a/k/a SS7), which allows carriers to connect so they can offer roaming and texting. According to Nohl, SS7 will be used for the next 10 to 15 years until its replacement (Diameter) is implemented, and Diameter is also vulnerable.

Representative Lieu admitted during the show that he has spoken with President Obama on that phone. After hearing the conversation, which was taped, he said, "First, it's really creepy. And second, it makes me angry." Following the revelation, Lieu asked the House Oversight Committee to investigate the vulnerability. Well it is a matter of national security, isn't it?

The Federal Communications Commission announced on Wednesday that it too will begin a study of mobile carriers' use of SS7, which has been used for decades and has reached its end of life.

Nohl has publicized the vulnerability since 2014, and the telecom carriers responded by providing alerts regarding the vulnerabilities and ways to fix them. But the message from the program is that all cell phones are vulnerable, and we can all be the victim of spying and someone listening to all of our telephone calls.

I still have a landline and I use it. Although only marketers tend to call me on my landline, I am becoming more and more a believer of using landlines again in homes and offices. A couple of weeks ago, when alerting everyone to sophisticated phishing schemes, I advised to pick up the phone and

call the boss to see if s/he really wants you to email those W-2s. The phone on your desk still works. And it is secure—probably more secure than a cell phone. So instead of relying on email or a cell phone, verify strange requests with your landline—the old way.

So why are landline telephones almost extinct, particularly when it appears they may be the answer to many security issues? The telephone companies want to limit or remove them because the lines are so expensive to maintain.

Thirteen states in the past three years, including Maine, have allowed telephone companies to stop providing traditional basic telephone services to consumers (i.e. landlines). Ever try to get cell service in Maine or New Hampshire? Oftentimes in remote areas the message is "no service." So if you don't have the ability to get a landline, and you don't have cell phone service, how can you call an ambulance, the police, or the fire department in an emergency?

That is the concern of the AARP and other consumer groups, as many elderly individuals do not have cell phones, do not get cell phone service, and will have no way to communicate in rural areas if they are unable to keep their landline.

So the conundrum is that landlines are arguably more secure than cell phones, and picking up the telephone is an important security risk management tool, but landlines are becoming extinct.

The Privacy Tip? Use your landline. It's probably a more secure way to communicate these days because hackers aren't concentrating on them at the moment. And hopefully the telephone companies and state regulators can figure out a way to keep landlines in existence for consumers in a manner that is reasonable to the telephone companies. It may be a matter of national security.

— 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.