October 22, 2015

DATA BREACH

CIA Director's Email Account Hacked

An anonymous hacker has contacted the *New York Post* to explain how he was able to hack into the CIA Director's AOL email account. According to several reports, a high school student and his two friends implemented social engineering to obtain credentials to hack into the personal account.

How did they do it? According to the hacker, he and his friends completed a reverse lookup of the Director's cell phone number to determine which telecommunications provider he used. Then they called that provider, saying they worked for the provider and were working with a customer they couldn't assist because they couldn't access the company database as it was down. They provided a fake Vcode and were then provided with the Director's account number, four-digit PIN, the backup mobile number on the account, his email address and the last four digits of his bank card.

Armed with that information, the hackers called AOL and complained that they were locked out of their account. Typical security questions were asked such as the last four digits of the bank card, and they were able to reset the password. They obtained access to the account and read emails, including emails the Director sent to his personal account from his government account.

While in his account for three days, they report that they were able to obtain a portion of his contact list, a spreadsheet listing the names and Social Security numbers of some US intelligence officials, his own application for top-secret security clearance, and a letter regarding interrogation techniques. The hackers posted redacted pages of the documents on Twitter.

The account has been disabled and the FBI and other agencies are investigating.

— Linn Foster Freedman

Sony Will Pay up to $4.5M to Settle Data Breach Case with Employees and up to $3.49M in Attorneys' Fees for Plaintiffs' Attorneys

Sony Pictures (Sony) agreed on Monday (October 19, 2015) to pay at least $2M and up to $4.5M to employees whose personal information was breached and posted online during the massive hack that hit Sony in 2014. The $2M is to cover claims of time and effort expended to prevent fraud and identity theft, and two years of identity protection for those affected, which includes identity fraud insurance. The

additional $2.5M will cover identity theft losses that are not covered by insurance.

The deal also includes up to $3.49M in attorneys' fees, compared to only $34,000 for the individual active settlement members. Wow.

— Linn Foster Freedman

DATA PRIVACY

EU Safe Harbor Update

A lot has happened since the European Court of Justice's declaration that the EU-US safe harbor framework is invalid (see related post).

First, the Article 29 Working Party, an organization comprised of representatives from each data protection authority in the EU, issued a statement late last week indicating that since transfers relying on safe harbor are now unlawful, companies transferring EU citizens' data to the U.S. may use the EU Standard Contractual Clauses or Model Clauses and Binding Corporate Rules on an interim basis until negotiations over a new safe harbor framework are complete. Further, it declared that if a new framework cannot be agreed upon by the end of January, 2016, it will exercise the powers vested in them to investigate complaints and enforce violations.

Second, the Irish High Court asked the country's Data Protection Commissioner to investigate Facebook to determine whether the personal data of EU Facebook users was properly protected when transferred to the U.S.

Third, Israel's data protection authority this week declared "[p]ursuant to the European decision, it is no longer permissible to rely on the safe harbor as a basis for transfers of personal data from Israel to the U.S." It further announced that it "will publish information and additional clarifications if necessary."

And finally, on Tuesday the U.S. House of Representatives passed the Judicial Redress Act, which (if enacted) would give citizens of foreign countries covered under data sharing agreements with the U.S. the ability to sue the U.S. government for privacy violations if their information is shared with the U.S. for law enforcement purposes. This was one of the reasons cited by the European Court of Justice in striking down the safe harbor framework. It brings the U.S. in line with its allies, who allow U.S. citizens redress for privacy violations in other countries.

We anticipate that there will continue to be a flurry of activity around the safe harbor framework. We will continue to update you on developments as they occur.

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

What is a Federal Computer Crime? It Depends On Where You Are

When an employee has access to data for work, but the employee uses it for nonwork purposes, is that a federal crime under the Computer Fraud and Abuse Act (CFAA) (18 U.S.C. § 1030)? The answer depends on where you are.

Ninth Circuit & Fourth Circuit: No, It's Not a Crime

In late August, the Ninth Circuit Court of Appeals vacated convictions of two LA police department officers under the CFAA in *U.S. v. Christensen*, No. 08-50531, Slip Op. at 32 (9th Cir. Aug. 25, 2015). The officers had allegedly searched confidential police databases for use in an unauthorized private detective ring. The court ruled this was not a crime under the CFAA.

The court reasoned that CFAA, which it sees as an "anti-hacking statute," is "limited to violates of restrictions on access to information, and not restrictions on use." *United States v. Christensen*, No. 08-50531, Slip Op. at 32 (9th Cir. Aug. 25, 2015) (quoting *U.S. v. Nosal*, 676 F.3d 854, 864 (9th Cir. 2012) (en banc)). The court noted "Congress has created other statutes under which the government employee who abuses his database access privileges may be punished, but did not intend to expand the scope of [CFAA] the federal anti-hacking statute." Slip Op. at 34-5.

The Fourth Circuit has taken a similar view of the CFAA. See *WEC Carolina Energy Solutions v. Miller*, 687 F.3d 199 (4th Cir. 2012).

Other Courts: Yes, It Is a Crime

Other U.S. Courts of Appeals have applied a broader reading of the CFAA, arguably ruling that it applies to employee misuse of corporate information. See EF *Cultural Travel BV v. Explorica, Inc.*, 274 3d 577 (1st Cir. 2001); *U.S. v. John*, 597 F.3d 263 (5th Cir. 2010); *Int'l Airport Ctrs. LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006); *U.S. v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010).

The Second Circuit: Considering the Issues

The Second Circuit continues to think about the issue. In *United States v. Valle*, 14-4396-CR, as we reported earlier, the court heard oral argument in May, but has not yet issued a decision. Most recently in September, the attorneys in *Valle* are arguing about what the Ninth Circuit's ruling in *Christensen* means in dueling letters to the Court.

Depending on how the Second Circuit comes out, misuse of employer information may be a computer crime under the CFAA in New York, but not in California. We will keep you posted.

— Nuala E. Droney

HEALTH INFORMATION

ONC Finalizes Interoperability Roadmap, Includes Milestones to Be Achieved by 2017

The Office of the National Coordinator for Health Information Technology (ONC) recently finalized the first version of its interoperability roadmap, Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap. The Roadmap describes the goals to be accomplished in order to reach nationwide interoperability by 2024. The first goal, to be completed between 2015 and 2017, is to "send, receive, find and use priority data domains to improve health care quality and outcomes." The second goal, to be completed between 2018 and 2020, is to "expand data sources and users in the interoperable health IT ecosystem to improve health and lower costs." The final goal, to be completed between 2021 and 2024, is to "achieve nationwide interoperability to enable a learning health system, with the person at the center of a system that can continuously improve care, public health, and science through real-time access."

The Roadmap focuses on the milestones, action items and commitments necessary to achieve the 2017 goal. These include organizations ensuring that health IT is developed and deployed in a secure manner, with encryption for all data at rest and in transit. In addition, the ONC aspires for at least 65 percent of health care organizations to offer secure portals for patients to access their health information by 2017. In furtherance of this milestone, the ONC intends to establish best practices for identity authentication.

In January 2015, the ONC released a draft of the roadmap and requested public comment. The final Roadmap incorporates comments from over 250 organizations. Karen B. DeSalvo, National Coordinator for Health Information Technology, stated that the Roadmap is "a living document, and we intend to evolve it in partnership with the public and private sectors as technology and policy require." The ONC expects to update the Roadmap every two years.

— Pamela H. Del Negro

DRONES

DOT and FAA Hope to Release New Drone Registration Requirements Very Soon

"Registering unmanned aircrafts will help build a culture of accountability and responsibility, especially with new users who have no experience operating in the U.S. aviation system. It will help protect public safety in the air and on the ground." These remarks were made by U.S. Department of Transportation (DOT) Secretary Anthony Foxx earlier this week when he addressed the DOT's goal of establishing rules for drone operator registration with the Federal Aviation Administration (FAA). The DOT plans to create a task force consisting of industry and government officials who will submit a report on registration requirements by November 20 to the DOT.

These registration requirements come not only after the FAA has been repeatedly urged to come up with a set of safety (and privacy) regulations for drone operations, but also after the FAA has seen a sharp increase in the number of reported pilot drone sightings, increasing from 238 in 2014 to 650 halfway through 2015.

The FAA anticipates a speedy process for pursuing regulations after the submission of the November 20th report. FAA Administrator, Michael Huerta, said, "Registration will help make sure that operators know the rules and remain accountable to the public for flying their unmanned aircraft responsibly." Of course besides determining the specifics for registration, the task force will determine which types of drones should be excluded from these requirements, such as toys—maybe the idea is to get these registration requirements out before kids start flying their new unmanned aircrafts this holiday season. We will keep you posted on the details of the task force's report and any subsequent regulations.

— Kathryn M. Rattigan

CYBER SECURITY

Chinese Government Arrests Hackers

We have been reporting on the success of the Department of Justice in combatting cybercrime through prosecutions of hackers. But we never expected this. Following Chinese President Xi's visit to the U.S., and for the first time in years, the Chinese government has arrested several alleged hackers at the request of the U.S. government. The hackers reportedly stole highly sensitive IP data from U.S. corporations. U.S. intelligence officials and law enforcement agencies apparently gave the Chinese government a list of hackers and requested that they be arrested, and lo and behold, several of them

have indeed been arrested.

Whether they will be prosecuted or not will be seen. But baby steps are better than no steps at all in the fight against theft of trade secrets of U.S. companies.

— Linn Foster Freedman

New York Stock Exchange Releases Cybersecurity Guide for Public Companies

We continue to urge CEOs and boards of public companies (and private and not-for profits) to harken the call of getting a handle on cybersecurity risk to companies today. Not too soon, the New York Stock Exchange published a book this week entitled "*Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers Provides Actionable Advice and Best Practices.*"

The 355 page book includes discussion of board obligations and action plans, improving questions asked by CEOs, trade secrets, data breaches, incident response and consumer protection.

A definite read for CEOs and board members who are struggling to understand cybersecurity risk, response, preparedness and action.

— Linn Foster Freedman

Department of Energy Invests $34M in Cybersecurity for Critical Infrastructure

The Department of Energy (DOE) has announced that it will invest $34M to the University of Arkansas and the University of Illinois for two projects designed to "improve and enhance" the protection of the U.S. electric grid, and oil and natural gas infrastructure from cyber threats. The DOE stated, "To meet this challenge [cybersecurity], we must continue investing in innovative, next-generation technologies that can be transitioned to the energy sector to reduce the risk of a power disruption resulting from a cyber incident."

The university teams will include experts of engineering power systems and computer science relating to cybersecurity.

— Linn Foster Freedman

PRIVACY TIP #6

Protecting Your Child's Identity

I have spent some time over the past few weeks concentrating on steps individuals can take to protect their privacy and identity. But how do you protect your child's identity?

In some ways, the same way you protect your own. But keep in mind that in many instances, if a child's identity is stolen, it is very difficult to find out. It doesn't matter to identity thieves whether an individual is an adult or a child. If they get enough personal information, including a Social Security number (SSN),

they can wreak havoc on anyone.

Here are 10 basic tips to take into consideration to protect your child's identity:

1. Don't give your child's Social Security number to anyone unless it is required. Don't give it to your pediatrician, to the day care center, to summer camp, or to the school (unless you are applying for aid or a loan). There is no reason why any of these entities need your child's Social Security number. Just say no. And don't carry your child's SSN in your wallet (nor your own).

2. If you have to give your child's SSN, find out what privacy and security protections are taken by the entity to protect it, and read its privacy policy. Who do they share your child's data with and how can you request restrictions on disclosure? You can't get out of giving it to the IRS and usually your employer's benefits providers request it for benefits (although I wish they would get away from requesting full SSNs), banks for custodial accounts (to comply with the U.S. Patriot Act) and for older children, the common college application (again, this is frustrating as it is questionable why they need the full SSN). Read the fine print and opt out of sharing with third party entities.

3. If you can request restrictions, do so. For instance, if you open a custodial bank account for your child at your bank, the bank is required to send you a notice of how they will use your child's personal information and who they will share it with under the Gramm–Leach-Bliley Act. Call the number on the notice and request restrictions on disclosure of your child's personal information (including SSN) to the fullest extent you are able. There is really no reason why you should want your child's personal information to be shared with all of the bank's marketing firms.

4. If your child's personal information has been breached, such as in the recent data breaches of Anthem or Excellus, do the same thing you do for yourself. Sign up for any credit monitoring or fraud resolution products or services for your child. Be vigilant and suspicious if you get calls from credit card companies or collection agencies.

5. Get a free copy of your child's credit report to assure your child doesn't have one. A credit report can be requested from each of the three credit bureau—Experian, Equifax or Transunion. If your child has a credit report (most children shouldn't have one), contact one of the credit bureaus to correct any fraudulent information on the credit report.

6. If your child has a credit report and shouldn't have one, consider placing a fraud alert and/or credit freeze on your child's accounts to ensure that no more accounts can be opened in your child's name with his/her SSN while you resolve the identity theft.

7. Be sure to check your child's credit report before he/she gets an apartment, applies for a car loan or has to put down a deposit for utilities. It is better to have anything cleared up before it becomes an issue.

8. Shred any and all documents that have your child's personal information (including SSN) on it.

9. Be educated and wary about the information you provide to your child's school and request the school's privacy and security policies, including the administrative, technical and physical safeguards the school takes to protect your child's information. Most schools must comply with the Family Educational Rights and Privacy Act (FERPA), which allows you the right to opt out of sharing certain information with others.

10. Teach your children how to protect their information and their identity. Make it a priority so they are educated and aware of the risks the digital world poses to them and so they can protect themselves as they mature. This includes their online behavior, social media disclosures, information sharing through

mobile apps and their smartphones. All of that information will follow them the rest of their lives. The pictures aren't polaroids and can't be destroyed and there is no "delete" button.

— 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.

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

---