May 26, 2016

DATA BREACH

[O'Charley's Diners Warned of Payment Card Data Breach]

Diners who used credit and debit cards at the Tennessee based O'Charley's restaurants between March 18, 2016, and April 8, 2016, were notified by O'Charley's of a data breach that affected its point of sale systems. Consumers were also warned by the Georgia attorney general, who suggested that consumers who dined at the chain monitor credit card and bank statements.

O'Charley's operates more than 200 restaurants in 17 states, including Georgia. O'Charley's announced that it has notified law enforcement. At the present time, it does not know how many cards were affected but has set up a website to assist consumers with precautionary steps: http://www.ocharleys.com/protectingourguests.

— Linn Foster Freedman

[Noodles & Company Alerts Customers of Credit Card Compromise]

According to Noodles & Company (Noodles), it received information from Visa that Visa cards used by customers at its fast-food chains since January have "possibly" been compromised. It is presently investigating unusual activity reported by Visa, is working with law enforcement, and has brought in a forensic firm to assist with the analysis.

This may be another in a long line of retail chains that have suffered a compromise of their point of sale systems over the past two years. Noodles is reportedly in the process of transitioning to chip cards, but apparently, they didn't transition quickly enough to avert a "possible" data breach.

— Linn Foster Freedman

[Milwaukee Bucks Become Latest Victim to W-2 Phishing Scheme]

We have been repeatedly warning our clients and readers about the massive and successful W-2 phishing schemes where hackers impersonate the CEO or CFO and send emails to payroll and/or HR folks in their companies requesting W-2 forms of employees [see related posts here and here].

It became such a problem that the IRS issued an alert to all payroll and HR departments on March 4, 2016, warning all industries about the pervasive problem.

The latest victim is my childhood hometown team, the Milwaukee Bucks. The phishing scheme involved was exactly like all the others—it impersonated the team president, Peter Feigin, requesting W-2 forms for employees. The W-2s were then sent to the hacker and the information of those employees, including their Social Security numbers were compromised.

The Bucks are providing the affected employees with three years of credit-monitoring services and identity restoration services.

We continue to see these phishing schemes successfully implemented, which underscores the continuing need to train employees and provide them with education and tools to feel comfortable to pick up the phone to confirm an odd request, such as the CEO requesting W-2s forms of employees.

— Linn Foster Freedman

Experian Sponsors Ponemon Study on Data Breach

Experian Data Breach Resolution sponsored a recently released Ponemon study entitled “Managing Insider Risk through Training & Culture.” The report is quite timely in light of all of the recent successful W-2 phishing schemes.

The report is very informative and worth the read. The highlights include that 66 percent of the respondents “admit employees are the weakest link in their efforts to create a strong security posture.” 55 percent of the respondents stated that their organization suffered a security incident of a data breach due to a malicious or negligent employee.

The top two risks cited by respondents in the study include a data breach “caused by a careless or negligent employee who exposes sensitive information or succumbs to a targeted phishing attack.” The companies also indicated that they have concerns over employees who could allow malware to infiltrate their system from an insecure website or mobile device and use unapproved cloud or mobile applications to send sensitive company information outside of the company.

Despite these concerns, the study found that only 35 percent of those surveyed confirmed that executives believed that data security training is a priority for the company. And only 50 percent believed that the training programs in place actually help change behavior. The training programs are deemed ineffective and don’t provide education on phishing and social engineering, mobile device training, or the use of secure cloud services. Shockingly, only 45 percent of those surveyed said their companies have mandatory training requirements.

Bottom line? Every organization is at risk (as we have continually seen over the past year with phishing attacks), and employees continue to be one of your top risks. Training, real training that gives employees valuable data security education and tools to be vigilant during the work day while using an organization’s computer assets or mobile technology, is essential in reducing the risk of data loss. Online training can be very boring and allows employees to multitask. Live training is much more effective and fun, and mixing in personal tips along with risks to the company is invaluable.

Effective training will get all employees to start looking around them, finding the keys to the filing cabinets, putting sensitive documents away at night, being more aware of using encryption for emails, and picking up the phone when the CEO is requesting W-2s of employees.

Effective employee training is essential for a company's risk management program, and the return on investment is invaluable.

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

PayPal Reaches Settlement with Texas AG over Privacy and Security Disclosures

PayPal agreed to pay $175,000 and strengthen its privacy and security disclosures in a settlement agreement reached with the Texas Attorney General's Office (AG's office). The AG's office claimed that PayPal failed to explain to users of its Venmo mobile money transfer app how users' personal information would be used and shared.

PayPal acquired Venmo in December 2013. The AG's office had been investigating whether Venmo had violated the Texas Deceptive Trade Practices Act. The investigation stemmed from allegations into whether the app used consumers' phone contacts without an explanation as to the purpose of the contacts or whether contacts would be shared. Based on the allegations, the AG's office argued that users of the app may have unknowingly shared private information regarding payments publicly.

The settlement agreement specifically requires PayPal to cease accessing Venmo users' contact lists absent prior disclosure of the type of information that will be accessed, the specific ways in which it will use the data, and how to use and disable certain features of the app that could compromise users' privacy. The investigation marked the manner in which state and federal authorities are taking measures to assist their citizens from inadvertently compromising their data privacy as they avail themselves of apps meant to simplify consumer transactions.

— Rachel V. Kushel

DATA SECURITY

Senate Hearing Reviews Ransomware in a School System

On May 18, the Senate Judiciary committee's Subcommittee on Crime and Terrorism heard from Charles C. Hucks, the executive director of technology for the Horry County, South Carolina School System. The 52 schools and the central offices in the system were all affected when the decision was made to shut down over 600 servers district-wide because of a spreading ransomware attack. While the school system had dealt with smaller ransomware attacks, its administrators were unprepared for the manner in which this one spread. According to Mr. Hucks, the 43,000 students and 3,800 faculty are highly dependent on technology, and this attack caused significant disruption. The Horry County School System eventually paid $10,000 (up from the $8,500 originally requested) in Bitcoin to receive the keys to unlock their servers. Within hours, the files and systems were decrypted and restored. On May 16, Senator Sheldon Whitehouse (RI) and Senator Linsdey Graham (SC) introduced the Botnet Prevention Act, which would give law enforcement greater powers to tackle botnets. Botnets are large groups of computers that have been taken over by malicious parties and distribute malware, ransomware, and spam or carry out other types of computer attacks. Senator Richard Blumenthal (CT) is a co-sponsor of the bill. Justice Department official Richard Downing testified in favor of important provisions of the bill.

— Richard M. Borden

SSO – Single Sign-On

Due to recent high-profile data breaches, users have a heightened awareness of security and how they manage or don't manage their various account credentials. People are beginning to pay more attention to the advice given to them by security professionals: advice regarding using strong passwords, using a different password for every account, and so on. Inevitably, a user will come across an advertisement for an SSO product and go to their IT Department requesting the implementation of SSO, saying "It's the answer to our endless list of passwords."

Well, kind of is the real answer. SSO breaks down into two basic types: enterprise SSO and account credential management. Enterprise SSO provides authorization and access across multiple systems, each of which has its own security layer. Starting with a directory server, typically Active Directory, or another Lightweight Directory Access Protocol (LDAP)-compliant directory, identity information can be shared in a variety of ways. Integrated Windows Authentication is a term used to refer to several different Microsoft protocols, Kerberos, SPNEGO, and NTLMSSP that allow for cross-system authentication. Security Assertion Markup Language (SAML) is an XML based method for exchanging identity information between a directory and web-based service. Finally, if an integrated method cannot be used, there are many third party SSO and identity management tools that can be implemented in the enterprise. Beyond helping to alleviate user password fatigue, implementing a SSO solution can provide increased security control and auditing capabilities. It can also be leveraged to assist in the implementation of Role Based Access Control (RBAC), which I discussed in a previous post.

Account credential management applications are also often referred to as SSO solutions. These are typically applications installed at the workstation level that gather and maintain account credentials and auto insert them for the user when it recognizes credential fields in a system or application. Such applications typically only require the user to authenticate against its account, thus the single sign on. Be aware, however, when selecting which SSO application to use. If it is cloud-based, be sure the provider is utilizing proper security. If is completely workstation-based, be sure the application has a way to back up your credentials should you change computers for whatever reason.

— Sean C. Lawless

DRONES

Voluntary Best Practices for Drone Privacy Finally Released

It's here! Last week, privacy groups and industry stakeholders that were participating in the National Telecommunications & Information Administration (NTIA) Multi-Stakeholder process released a set of best practices for commercial and private drone use. Participants included Amazon, AUVSI, the Center for Democracy and Technology, the Consumer Technology Association, CTIA, FPF, Intel, X (formerly Google X), New America's Open Technology Institute, PrecisionHawk, SIIA, the Small UAV Coalition, and many media organizations.

The best practices consist of the following:

- Inform others of your use of drones (i.e., where reasonable, provide prior notice to individuals of the general timeframe and area where you may anticipate using a drone to collect identifiable

data).

- Show care when operating drones or collecting and storing personally identifiable data (i.e., retain only information that you must retain and de-identify information when possible)
- Limit the use and sharing of identifiable data.
- Secure identifiable data.
- Monitor and comply with evolving federal, state, and local drone laws and regulations.

The full set of best practices is available here.

— Kathryn M. Rattigan

CYBERSECURITY

Brown Cybersecurity News Podcast: Rise of the Third-Party Vendor Threat

Last month, the Ponemon Institute released a report, Data Risk in the Third-Party Ecosystem, that confirmed what many suspected: third-party vendors are the wild, wild west of cybersecurity. A shocking number of companies surveyed do not believe that a third-party vendor will notify them if a data breach occurs, and even more doubt they'll be notified about a downstream breach.

In the podcast, Linn Freedman, Robinson+Cole partner and Brown University Executive Master in Cybersecurity professor, confirms that the survey corresponds to her professional experience as chair of Robinson+Cole's Data Privacy + Security team. She states, "We're seeing more and more data loss from third-party vendors, as opposed to companies. We're also seeing a break in the communication between the company and their third-party vendors."

We invite you to listen to this podcast to hear Freedman's insights into the magnitude of this threat, the role Target's HVAC vendor played in their notorious breach, and best practices for a vendor management program—auditing, contractual provisioning, corporate responsibility, and other related topics.

• Listen to the podcast.
• View the podcast transcript.
• Learn more about the Brown University Executive Master in Cybersecurity.

INTERNET OF THINGS

CDT and Fitbit Report on Wearable Health Tracker Devices

Last week, the Center for Democracy & Technology (CDT), through the cooperation of Fitbit, Inc. (Fitbit), released new guidance about wearable health tracker devices called "Toward Privacy Aware Research and Development in Wearable Health." Here are the most important takeaways of this report:

- "Internal research and development offers a unique window into data practices and policies at companies, such as insight into how data is categorized in projects, the way teams are structured, and the privacy and security methods that are deployed. Internal R&D also offers a flexible environment for piloting privacy-protective and ethical data policies and practices."
- "Building a culture of privacy, security, and ethics involves embedding practices and policies that place value on individual dignity and corporate data stewardship, and also prioritizes

contributions to the social good."

- "Technology companies are managing several dimensions of trust through internal research and development— the company and its users, the integrity of internal policies and practices for employees, and the relationship between the company and society. Successfully navigating this trust through practical measures must be at the core of any policy or practice recommendation."
- "Research departments at wearable companies face ongoing ethical questions related to the data they process. Policies and procedures around the uses of internal data, such as employee information, should be developed first."

In this report, CDT takes a close look at the practices and procedures within internal research and development teams of wearable device companies (Fitbit in particular), and pulls together the information collected through interviews, surveys, and other research to build a source for the industry's best practices and technology trends. Read the full report for more details on best practices for consumer privacy and internal research procedures.

— Kathryn M. Rattigan

GUEST AUTHORS

This article, courtesy of guest blogger Professor Peter Margulies of Roger Williams University School of Law, originally appeared in the Privacy blog of The Lawfare Institute.

Madison at Fort Meade: Checks, Balances, and the NSA

When a group of civil society representatives and academics gathered at the NSA this past Thursday, it became clear—to me at least—that the NSA has taken the teachings of James Madison very much to heart. Of course, I'd be surprised if code breakers and computer mavens are actually spending their days parsing Federalist No. 51. But the thoughtful and engaged discourse of NSA officials exemplified a renewed commitment to Madison's wisdom that the best security against concentration of powers in one branch of government resides in giving each branch the "necessary constitutional means … to resist encroachments of the others." Ironically, a more insular approach to queries of data collected under national security authorities persists at the FBI, which has far more daily interaction with U.S. courts.

Exhibit A of the NSA's commitment to Madisonian principles was the clear respect agency officials had for the advocacy of Foreign Intelligence Surveillance Court (FISC) *amicus curiae* Amy Jeffress. Jeffress participated in the proceeding that yielded the recently released November 2015 FISC opinion upholding the constitutionality of § 702 of the FISA Amendments Act (FAA). My own extrapolation from the nod to Jeffress's efforts is that Congress, as it considers reauthorization of the FAA in 2017, should provide an even more robust role for a public advocate [see Steve's article here and Marty and Steve's post here].

The widespread view emerging from Thursday's civil society meeting was that the presentation of opposing viewpoints in court leads to better-reasoned judicial opinions. This is hardly a revolutionary view—indeed, it is fundamental to the virtue of deliberation that Hamilton attributed to judicial review in Federalist No. 78. But, historically, the FISC has proceeded almost exclusively in *ex parte* proceedings, with the government making its case and the FISC sometimes asking the government for more information and sometimes agreeing with the government's initial application. As a result, FISC opinions from the pre-Snowden era addressing the legality of surveillance programs were often conclusory, with relatively little in-depth analysis or consideration of opposing positions.

Critics of surveillance practice have long argued that the thin analysis in FISC opinions paved the way for broad readings of legal authorities, such as the Court's approval of the Section 215 domestic metadata program. This is not to reopen the question of Section 215's legality, which I have previously defended here. As Lawfare readers are aware, the USA Freedom Act [see Bart Forsyth's analysis] transferred

metadata collection to private telecommunications carriers, addressing many—but not all—of the critics' concerns. The critics' procedural point, however, is that the FISC's dependence on *ex parte* proceedings makes such broad readings more likely.

Judge Hogan's November 2015 FISC opinion upholding Section 702 is more comprehensive in its analysis. Judge Hogan started with the basics: In enacting 702, Congress barred the targeting under the statute of U.S. citizens, lawful residents (LPRs), and other persons physically located in the United States, all of whom are protected by the Fourth Amendment. Congress only permitted the collection of communications in which the target was a non-U.S. citizen or non-LPR reasonably believed to be located outside the United States.

In finding that Section 702 complies with the Fourth Amendment, Judge Hogan cited several limits that the NSA has imposed on how it uses U.S. person data that is incidentally collected under this provision. For example, the NSA does not query U.S. person data collected upstream, directly from Internet hubs, since that dataset is more likely to contain U.S. person information than is downstream collection (which is done by private carriers or Internet Service Providers pursuant to specific requests from the NSA). Moreover, government agencies only query the downstream Section 702 dataset for foreign intelligence information or evidence of a crime.

As the recent 2015 transparency report from NSA demonstrates, the authority is used sparingly: in 2015, the NSA used fewer than 5,000 U.S. person search terms to query the content of unminimized Section 702 communications (although pursuant to statute we don't know the number of FBI queries). In addition, the government will only introduce Section 702 evidence in a prosecution for an offense involving national security or a limited number of serious crimes. Moreover, as Judge Hogan noted, FBI queries unrelated to crimes involving foreign intelligence "rarely, if ever" yielded positive results. The requirement that virtually all FBI queries that result in access to Section 702 data be recorded as such curbs the risk that FBI analysts would pose queries for reasons unrelated to statutory criteria (such as ethnicity, religion, or political opinion).

That said, Judge Hogan's analysis of FBI querying procedure was insufficiently rigorous on three points. In each area, the FBI has fewer safeguards than the NSA. First, unlike the NSA, the FBI does not maintain a separate database for Section 702 data. According to the 2014 Section 702 report by the Privacy and Civil Liberties Oversight Board (PCLOB), the FBI tags Section 702 data electronically but includes this data in a broader database that also includes purely domestic data collected by the FBI pursuant to court orders or other legal authorities. Aggregating databases in this way makes it far more difficult to monitor who has access to the 702 data.

The FBI's practice of aggregating databases sets up two further problems not sufficiently addressed in Judge Hogan's opinion. Because the FBI aggregates Section 702 data and data collected under other authorities, it is currently not practicable to require FBI personnel to provide a written justification for Section 702 queries (Hogan opinion, p. 28). This is problematic if one wishes to curb undiscerning or indiscriminate queries of the Section 702 database. (The PCLOB urged in its Section 702 report that the NSA (but not the FBI) provide such justifications, and Judge Hogan's opinion confirms that both the NSA and the CIA have adopted the PBLOB's recommendation.)

Finally, the FBI uses a counterintuitive definition of the term "query" that excludes requests for unminimized Section 702 data made by FBI personnel not cleared for access to this data (probably because the restricted FBI employee, who may be a field agent outside of Washington, lacks the requisite training). In such cases, the FBI employee receives notice that the search has triggered a positive "hit" in Section 702 data, but a search filter bars access to the data itself. The restricted FBI employee can only gain access under the following conditions: (1) authorization of another FBI employee cleared for access, based on either, (2a) a reasonable probability that the data concerns foreign intelligence information or is evidence of a crime, or, (2b) the restricted employee's help in determining the data's compliance with 2a's criteria.

This counterintuitive definition gives the FBI too much latitude in declining to document searches of Section 702 data. My concern here is not with FBI access to Section 702 data per se—I agree that, to

efficiently "connect the dots" on terrorist plots, the FBI should have access to this information without prior judicial authorization. Requiring a court order as a condition for such access would unduly burden law enforcement. My principal concern is with properly documenting such access since diligent documentation will in itself limit indiscriminate searches. That's where the FBI's current practice falls short.

It may overstate the case to assert, as Liza Goitein does here, that the FBI's counterintuitive definition of Section 702 queries masks a substantial loophole in querying procedure. Judge Hogan credited the government's assurance that such situations are "very rare." Nevertheless, the failure to clearly label a search by a restricted FBI employee as a query undermines transparency under Section 702. While secrecy is both inevitable and necessary in gathering foreign intelligence, a hard-won lesson learned in the wake of the Snowden disclosures is that lack of transparency reduces the perceived legitimacy of intelligence collection programs. To minimize this negative perception, the FISC should require more transparency in the FBI's documenting of queries (and Congress should mandate it in the 2017 reauthorization).

These concerns, while they should have prompted further analysis by Judge Hogan, are too minor and ministerial to call into question the court's holding that Section 702 is consistent with the Fourth Amendment. (District judges in the Second and Ninth Circuits have reached similar conclusions—see here and here.) Tellingly, these points also do not address the NSA. The NSA's querying protocol is more precise and exacting than the FBI's. While both the FISC and Congress should ensure that the FBI is subject to comparable procedures, that issue does not diminish Judge Hogan's diligence in addressing the NSA's safeguards.

Even in the absence of an *amicus* making opposing arguments, Judge Hogan may well have engaged in the comprehensive analysis of NSA safeguards that distinguishes his opinion. However, it seems logical to infer that the cogency and diligence of Jeffress's advocacy encouraged careful analysis from the court. That careful analysis, as well as the prospect of future *amicus* input, in turn may restrain future government requests for unduly broad readings of statutory collection authority. Hamilton, in Federalist No. 78, posited that judicial review would have this salutary *ex ante* effect. Of course, review should also not be unduly intrusive; for an insightful analysis of how oversight can strike this balance, see Privacy and Civil Liberties Oversight Board PCLOB member Rachel Brand's post.

When Congress takes up reauthorization of the FAA in 2017, expansion of the *amicus* authority in the USA Freedom Act into a full-fledged public advocate should be a cardinal topic of legislative deliberations. Notably, no one at Thursday's civil society conclave even remotely suggested that the involvement of a distinguished lawyer like Jeffress would risk disclosure of sensitive national security data. Similarly, a full-time public advocate, chosen from lawyers of a comparable pedigree, would pose no threat on this score. Moreover, the establishment of a full-time public advocate would promote public confidence in the resiliency of the NSA's internal constraints; any slippage in those safeguards would soon become known to the advocate, and then to the FISC and Congress. A public advocate might also exert a healthy influence on the FBI's query procedures, which require tweaking.

While the intelligence community might have to make minor adjustments, a diligent public advocate would not stifle the enterprise and ingenuity that we expect these agencies to show in "the common defence." A public advocate could assist Congress, the courts, and civil society in fashioning a conception of privacy that minimizes gratuitous or invidious intrusions while promoting both individual and general welfare (See Susan Hennessey's post).Thursday's gathering suggested that working within a framework of rules to accomplish this goal is integral to the NSA's mission. A public advocate would make these rules function more effectively.

Madison and Hamilton would not be surprised.

— Peter Margulies

PRIVACY TIP #36

Connected Car Security

A recent Government Accountability Office report outlined vehicle cybersecurity concerns, outlining that hackers can penetrate the technology of vehicles in both long-range and short-range attacks, including targeting Bluetooth controls. These car hackings allow the hackers to access steering, brakes, telematics, and critical controls of cars.

Just to put the threat in context, it has been reported that National Highway Transportation Safety Administration (NHTSA) publications indicate that a modern luxury vehicle includes up to 100 million lines of software code. This is in contrast to a Boeing 787 Dreamliner that has approximately 6.5 million lines of software code. What does that mean? The more lines of code, the more vulnerabilities and openings for hackers to get into.

Hence comes the recent warning by the FBI: treat your car like you would treat your computer, your laptop, and your phone when it comes to data security. Many drivers have no idea how much data a car has and stores. Cars are now connected to the Internet, and drivers are using GPS in their car (like location-based services on your smartphone), connecting apps to their cars and streaming music, and cars are recording drivers' driving habits, including speed, braking, and erratic movement.

The FBI says that car hacking is a real risk that you should treat your car just like you would any other connected device. Limit access to your vehicle to protect it from an unauthorized person infecting your car with malware, be careful about the apps that you use through your car and what information you are providing to them, keep vehicle software that you receive from the manufacturer up-to-date, and don't make modifications to the vehicle software.

We don't think of our cars in the same way as we do our laptop or phone, but they are just a bigger version storing a tremendous amount of personal data. Be aware of the data that your car has and protect it like any other connected device.

— 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. Following, are several upcoming speaking engagements:

- June 7 – The Quorum Initiative Cyber Intrusions event in New York City (Linn F. Freedman)
- June 8 – The Quorum Initiative Cyber Intrusions event in Washington D.C. (Linn F. Freedman)
- June 21 & 22 – Cloud Financial Services USA Conference in New York City (Richard M. Borden)
- 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.