Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

March 10, 2016

CYBERSECURITY

Maritime Industry Beware: Hacking Pirates Are Targeting Valuable Cargo

As I have written before, I am a big fan of the sharing of cyber intrusion information so all industries can learn from one another. No industry is immune from cyber-attacks.

But this is a new one, and good to know for the maritime industry. The Verizon RISK team reports that a shipping company hired the team on multiple occasions to investigate the loss of valuable cargo that had been targeted by tech savvy pirates. The pirates were able to hack into the ship's system to determine where the valuable cargo was located on numerous ships and then steal it when the crew came ashore. When the losses began to mount up, the Verizon RISK team was hired.

Although the Verizon RISK team was reportedly able to track the hacking through the ship's logs, and determine the attack was unsophisticated, the result was significant for the shipping company, which lost valuable cargo on multiple occasions.

Ships are loaded with computer systems that need to be protected like any other industry. The maritime industry is at risk and may consider placing data security high on the priority list.

— Linn Foster Freedman

FAA Calls for Contractors to Assess Airplane Cyber-Threats and Vulnerabilities

The Federal Aviation Administration (FAA) is now reaching out to contractors to help assess cyber-attack threats and vulnerabilities to communications systems on airplanes. This new effort is part of the Aircraft Systems Information Security/Protection initiative. The FAA says that this initiative's goal is to develop "aviation policies, regulation, and training requirements to ensure the resilience of aircraft network systems from cyber-attacks."

The FAA is asking that contractors prepare an outline for studying and tracking these vulnerabilities, which will hopefully lead to a complete risk assessment and eventual detection system for potential threats. Contractors will be awarded nine-month contracts but may also be asked to participate in the two subsequent phases over the next five years.

The FAA hopes to find out more information on the effects of the connections between planes and external networks like gate agents and whether these connections need better security protections. Of

course, this outreach comes after a 2015 U.S. Government Accountability Office report urging the FAA to take a stronger approach to cybersecurity.

— Kathryn M. Rattigan

ENFORCEMENT + LITIGATION

Home Depot Agrees to Settle Data Breach Class Action Suit for at Least $19.5 Million and Up to $28 Million, Including Attorneys' Fees

Home Depot announced on March 7, 2016, that it is agreeing to settle claims against it for the massive data breach that occurred in 2014, affecting up to 56 million debit and credit card holders for at least $19.5 million, and up to $28 million, including attorneys' fees and costs.

The settlement includes the payment of up to $13 million into the settlement fund, which will reimburse consumers for any out-of-pocket or unreimbursed costs and identity theft protection services for the affected consumers for 18 months, at an estimated cost of $6.5 million.

The settlement also includes the payment of attorneys' fees, not to exceed $8.475 million for the class action attorneys, and up to $300,000 in costs.

— Linn Foster Freedman

Bitcoin Traders Allegedly Bribe Pastor to Conduct Transactions

New York federal prosecutors allege in an unsealed indictment that Trevor Gross, a New Jersey pastor at Hope Cathedral and chairman of a credit union, was bribed $150,000 by illegal bitcoin traders to complete transactions for Coin.mx.

The unregistered bitcoin exchange was reportedly behind the hacking of a major bank that affected up to 83 million customers.

The indictment alleges that the bitcoin operators bribed Gross to use the credit union to process transactions. The pastor assisted them in getting named directors of the credit union and turned over control of the credit union to them to continue the illegal transactions. The credit union was liquidated in November.

Gross faces 30 years in jail for the charges.

— Linn Foster Freedman

Class Action Against Reader's Digest for Selling Subscribers' Personal Information

Reader's Digest, owned by Trusted Media, was hit with a class action in New York federal court alleging that the magazine sells its subscribers' personal information, including names, addresses, and demographic information, to data miners without any consent, in violation of the Michigan's Preservation

of Personal Privacy Act. Class representative, Shannon Taylor, claims that she received unwanted junk mail and telephone solicitations. The complaint states, “In addition to causing waste and inconvenience, direct-mail advertisers often use consumer information to lure unsuspecting consumers into various scams, including fraudulent sweepstakes, charities, and buying clubs.” The magazine allegedly allows third parties to buy mailing lists and send out these unwanted advertisements. Taylor claims that Reader’s Digest will sell its subscribers’ personal information “to anyone willing to pay for it.”

Subscribers are not required to read or agree to any terms of service, privacy policy or information-sharing policy. In addition to privacy violations, the class action asserts a claim for unjust enrichment.

— Kathryn M. Rattigan

Yahoo Refuses to Comply with Bankruptcy Judge’s Order to Turn over E-mail Account

Yahoo is objecting to a Delaware bankruptcy’s order to provide access to one of its email accounts, arguing that its compliance would violate the Stored Communications Act (SCA). At issue is a Yahoo email account purported to be maintained by a subscriber named Abdullah Rasimov. The Irish Bank Resolution Corp, Ltd., the debtor in the bankruptcy, claims that the Rasimov email account contains information supporting an alleged scheme by former billionaire Sean Quinn and his family to evade payment on $3.8 billion in loans.

After Rasmov failed to respond to an order requiring disclosure of his e-mails, the bankruptcy judge ordered that two IBRC representatives were the actual subscribers of the account. As a result, the Court ordered the e-mails be disclosed to IBRC.

Yahoo argued that the bankruptcy court’s rulings did not fall within the narrow exceptions of the Stored Communications Act. Additionally, Yahoo contended that the Court’s decision as to the identity of the actual subscribers of the e-mail account did not “in fact” render them the subscribers under the SCA.

The bankruptcy judge did not rule on Yahoo’s arguments presented at the March 1 hearing, indicating that he wanted to further research the matter. However, the Court did express some reservation with Yahoo’s position stating that e-mail accounts are routinely transferred in bankruptcy proceedings, and he is simply doing so by judicial order.

We will keep you apprised of developments as they arise.

The case is *In re: Irish Bank Resolution Corp. Ltd.*, case number 1:13-bk-12159, in the U.S. Bankruptcy Court for the District of Delaware.

— Brian J. Wheelin

DIGITAL ASSETS

Oregon and Wyoming Enact Model Digital Assets Law

Although numerous states have studied and introduced legislation adopting the Uniform Fiduciary Access to Digital Accounts Act, only three have adopted it.

The first was Delaware, which adopted the model digital assets law on August 12, 2015, effective

January 1, 2015.

Oregon became the second state to adopt the Uniform law, when the governor signed the SB 1554A, the Revised Uniform Fiduciary Access to Digital Accounts Act on March 2, 2016, effective January 1, 2017.

And finally, the governor of Wyoming signed its version of the Model Act on March 7, 2016, making it the third state to adopt the Model Act.

The Model Act allows heirs and personal representatives to have access to digital accounts left behind by deceased individuals. It streamlines the ability of the executor and personal representative to gather the digital assets and get access to them to administer the estate.

Providing a list of digital assets and the ability to access the digital assets are important parts of estate planning, and the model laws in these states will streamline the recovery of digital assets of deceased individuals in those states.

Other states are considering adopting the Model Act, and we anticipate seeing the passage of other state laws in this area.

— Linn Foster Freedman

Physical Therapy Provider's Patient Testimonials Lead to $25,000 OCR Settlement and Admission of Civil Liability

On February 16, 2016, the U.S. Department of Health & Human Services Office for Civil Rights (OCR) announced that it had entered into an agreement with Complete P.T., Pool & Land Physical Therapy, Inc. (CPT), a physical therapy practice located in California, to resolve HIPAA violations arising from CPT's impermissible disclosure of protected health information (PHI) on its website in the form of patient testimonials.

OCR initiated an investigation in 2012 and determined that CPT had impermissibly disclosed PHI on its website without obtaining HIPAA-compliant authorizations. Specifically, CPT posted patient testimonials, including full names and full face photographs, without obtaining valid authorizations from the individuals identified in the testimonials. OCR concluded that CPT violated HIPAA's Privacy Rule by failing to reasonably safeguard PHI, impermissibly disclosing PHI, and failing to implement policies and procedures designed to ensure compliance with the Privacy Rule's authorization requirements.

As part of the resolution agreement, CPT admitted civil liability for violating the Privacy Rule, agreed to pay $25,000, and entered into a three-year corrective action plan (CAP) with OCR. The CAP requires CPT to develop and implement written policies and procedures to ensure Privacy Rule compliance that include, but are not limited to, measures that address (i) permissible uses and disclosures of PHI and (ii) individual authorization requirements. The CAP also requires CPT to provide workforce training on its HIPAA policies and procedures, subjects CPT to heightened reporting requirements related to HIPAA violations, and obligates CPT to submit annual CAP-compliance reports. In addition to those conditions—which are standard in OCR corrective action plans—the CAP also requires CPT to remove all PHI from its website for which it does not have a valid HIPAA-compliant authorization by February 12, 2016.

For health care providers and suppliers subject to HIPAA, OCR's resolution agreement with CPT is particularly noteworthy for two reasons:

- CPT's failure to obtain valid authorizations from patients before posting their names and faces

on its website represents a straightforward violation of a basic HIPAA requirement that HIPAA-covered entities must be aware of, and comply with, especially in connection with marketing activities that utilize PHI

- CPT was required to admit civil liability for violating the Privacy Rule, a departure from previous OCR resolution agreements that customarily contain "No Admission" provisions explicitly rejecting any admission of liability. This appears to be the first time a covered entity has been required to admit civil liability as part of a resolution agreement and may portend a new approach by OCR to investigating and resolving HIPAA complaints.

— Conor O. Duffy

DATA PRIVACY

FTC Issues 9 Orders for PCI DSS Compliance Assessment Information

The Federal Trade Commission (FTC) issued orders to 9 companies at the beginning of this week, seeking information on how each company conducts Payment Card Industry Data Security Standards (PCI DSS) compliance assessments. PCI DSS audits are required by all major payment card-issuing companies of ALL retailers and business that process over 1 million credit card transactions per year. PCI DSS protects consumers' financial information by requiring minimum security measures when processing payment card data. The FTC is specifically seeking information about the way in which the assessors and companies interact, copies of a limited set of PCI DSS assessments themselves, and information on the other types of services provided by the companies (e.g., forensic audits). All information collected by the FTC will be used to put together a study on the current state of PCI DSS assessments. We will look for the study once it is released later in the year.

— Kathryn M. Rattigan

Brooklyn Heights Homes Will Close Their Doors to Tours: Another Victim of the Modern World

For over 31 years, the Brooklyn Heights Association (the Association) has offered tours of private residence brownstones, allowing the curious passerby the opportunity to see what's beyond those stoops. However, after over three decades of tours, the Association is closing its doors. Literally. And why? Well, the Association says that it has fallen victim to the times–Google, that is. Erika Belsey, vice president of the Association, explained, "The people who put their house on the tour, it's an unbelievable act of generosity, for they get no credit in a funny way, because its anonymous. Now you look at the address–you look it up, you find out everything. It's just an invasion of privacy in the way that it wasn't 30 years ago."

The tours occurred every May in five Brooklyn Heights homes for $40 per person. The rules were simple: no photographs and no children except babies. Volunteers were stationed in each room, on each floor, and on each landing, not only for safety but to assure that photographs were not taken. Now with smartphones, photos can be taken rather elusively, without even holding the phone within your vision. The owners are unaware of any photos popping up on social media, but the owners and the Association are being cautious. They are worried that the combination of the information available through a Google search and tour guests posting photos on social media could lead to more burglaries. For now, the doors are closed.

— Kathryn M. Rattigan

Virginia First State to Pass Fantasy Sports Consumer Protection Legislation

The new Virginia Fantasy Contests Act regulates consumer privacy on fantasy sports game websites, like DraftKings and FanDuel, and also requires fantasy sports companies to pay a licensing fee in Virginia to pay for the cost of oversight. The Virginia Department of Agriculture and Consumer Services will lead the oversight of these companies, including ensuring that all users of these fantasy sports sites are 18 years of age or older, that employees do not pass along confidential information (e.g., information that can affect the outcome of the fantasy contests), and that these companies segregate user funds from operational monies.

With more than 1.2 million fantasy sports players in Virginia each year, this will not only mean big responsibility for the oversight team but also more careful compliance by these fantasy sports companies. Other states are sure to follow Virginia's lead.

— Kathryn M. Rattigan

GUEST POSTS

Privacy Shield's Prospects: the Good, the Bad, and the Ugly

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

If the devil is in the details, then the announcement early Monday of the inner workings of the new US-EU data-transfer agreement, Privacy Shield, may lack the granularity the deal needs to flourish. There is much to applaud in the new agreement, including extraordinary transparency from the US and a new safeguard to address EU privacy complaints in the form of a State Department Ombudsperson. Those virtues, however, may not be sufficient to ensure the viability of Privacy Shield, which replaces the Safe Harbor framework invalidated by the Court of Justice of the European Union (CJEU) in *Schrems v. Data Commissioner*.

The CJEU struck down Safe Harbor on the grounds that it lacked both substantive and independent procedural protections against US intelligence collection. The Privacy Shield roll-out is short on concrete information regarding the State Department Ombudsperson's authority and is instead reliant on broad US "representations" regarding substantive limits on foreign intelligence collection. The CJEU may not be impressed, especially since the CJEU rarely provides European officials with the deference supplied by the European Court of Human Rights (ECHR).

First, the good in Privacy Shield: ODNI General Counsel Bob Litt's letter reinforces a salutary trend toward transparency that ODNI has championed since the Snowden revelations. To my knowledge, no intelligence service has provided close to the level of detail about intelligence community (IC) structure and decision making that the ODNI letter provides, as it builds on the commitment announced by President Obama in his PPD-28 initiative. The ODNI letter painstakingly describes several layers of review within the IC, including the setting of priorities by the National Signals Intelligence Committee (SIGCOM). In comparison, most European states continue to keep mum about their own internal processes.

The ODNI letter also reaffirms substantive limitations in PPD-28. Bulk collection abroad, which ODNI says may sometimes be necessary to "identify new or emerging threats" concealed in the forest of global

data, is limited to the grounds specified in PPD-28, including counterterrorism, combating weapons proliferation, addressing transnational illegality including sanctions evasion, detecting threats to US or allied forces, and learning about certain activities of foreign powers. The US also reiterates its PPD-28 pledge not to collect information in bulk for the purposes of suppressing dissent, disadvantaging individuals or groups based on criteria such as race, gender, or religion, or supplying US firms with a competitive advantage. Moreover, the IC cannot engage in the "arbitrary or indiscriminate collection" of data regarding "ordinary European citizens."

The ODNI letter commits the IC to tailoring collection. Analysts will focus on "specific foreign intelligence targets or topics through the use of discriminants (e.g., specific facilities, selection terms and identifiers)" whenever that specific approach is "practicable." Moreover, the IC has multiple layers of internal review, including the ODNI Civil Liberties and Privacy Office. I would add that my own conversations with ODNI and NSA privacy officials—who regularly engage with the public and the privacy community—reinforce my view that this internal control is indeed robust. Other constraints within the executive branch include inspectors general who report regularly to Congress, and the Privacy and Civil Liberties Oversight Board (PCLOB), which has authored well-received reports on U.S. surveillance. In addition, ODNI notes that the Foreign Intelligence Surveillance Court (FISC) now has statutory authority to appoint independent advocates, including noted privacy advocates. And, of course, Congress can also monitor the IC, exerting budgetary pressure if it sees something untoward. The FISC's authority to appoint independent attorneys stems from statutory changes, including the USA Freedom Act, negotiated with the Administration in the wake of Snowden's disclosures.

That's the good in the Privacy Shield roll-out; now for the bad. First, the US representations that it won't engage in "arbitrary or indiscriminate" collection on Europeans are described only in general terms. The European Commission (EC) statement that the new framework has "adequate" protections for Europeans relies on "explicit assurances" provided by the US. However, the EC statement shares nothing on what those assurances entail. Since the US and the EC have significant business interests dependent on a new privacy agreement, some may question whether those assurances are as robust as the CJEU or EU privacy regulators would prefer. There is simply no way to judge, based on the materials disclosed thus far.

Moreover, the ODNI letter does not address a central EU concern with the status quo: the vagueness of the "foreign affairs" basis for collection under section 702 of the Foreign Intelligence Surveillance Amendments Act (for more, see Tim Edgar's analysis). I've written previously that the foreign affairs prong of section 702 is limited by language that confines such collection to matters concerning a "foreign power" or "territory." I continue to believe that this language focuses the foreign affairs prong on collection relating to foreign officials and does not extend to monitoring of foreign persons' routine activities. Perhaps the assurances that US officials provided to the EC confirm this view. Moreover, perhaps the FISC can provide a check to unduly broad interpretation of this provision, since the EC adequacy analysis states that the IC has agreed to a PCLOB recommendation to provide the FISC with a random sample of analysts' tasked searches. However, the lack of public reassurance on this score underlines a concern of the EC Working Group that the CJEU highlighted in *Schrems*.

Furthermore, procedural safeguards outlined by ODNI may not be as robust as the CJEU wishes. The inspectors general, for example, are hampered by a recent Justice Department Office of Legal Counsel opinion that allows executive branch agencies to limit disclosure of data to inspectors general conducting investigations. Moreover, the FISC has no control over the United States' biggest foreign collection program, which is based on Executive Order 12333. The State Department Ombudsperson may have the authority to address complaints that involve EO 12333, but the announcement is not clear on this point. The Ombudsperson description in Annex III of the roll-out says that this official will "work closely" with other government officials. Nevertheless, the description does not specify that the Ombudsperson will have full access to IC data and procedures.

Similarly, according to the EC statement, the Ombudsperson will have to "confirm" that each complaint received has been "properly investigated." To confirm this, the Ombudsperson must ascertain that surveillance has complied with US law, including the "representations" and "explicit assurances" that the US has provided, or that any violation has been remedied. However, this confirmation brings us back to

the lack of specificity in the public version of those US "representations." It is difficult to see how robust the Ombudsperson's review will be, when so much depends on assurances that are not accessible to the public, the CJEU, or European data regulators.

As Privacy Shield is implemented, the Ombudsperson may develop a course of dealing with the IC that addresses these concerns. Experience might demonstrate that the Ombudsperson has access to all the information that she needs, and uses that information to keep the IC honest. But that experience will be outside of the four corners of the Privacy Shield's founding documents, making consideration of experience's teachings a tougher sell with skeptical actors such as the CJEU.

That brings us to the ugly. The CJEU should provide some deference to the EC, particularly on matters involving national security. That deference is apparent in decisions of the ECHR on surveillance, such as *Weber v. Germany*, which upheld a substantial overseas surveillance program conducted by the German Republic. However, the CJEU has in practice diminished deference to near-microscopic levels in cases like *Schrems* and *Kadi v. Council*, which invalidated the EU's implementation of the UN's terrorist sanctions framework. Indeed, the framework invalidated in *Kadi II* also involved an ombudsperson, who had been effective in ensuring fairness to subjects of sanctions. This real-world efficacy made no difference to the CJEU. Instead, the CJEU insisted on a more formal due process mechanism, which was unworkable because of states' reluctance to disclose intelligence sources and methods supporting terrorist designations.

The CJEU may also have concerns about the independence of the State Department Ombudsperson for Privacy Shield. True, that official will not formally be part of the IC, and in this sense will be independent. Nevertheless, the State Department is also an executive branch department, and is a customer of the IC, making use of intelligence that the IC provides. The President can fire the Ombudsperson, as he or she can fire IC officials. The Ombudsperson may as a practical matter retain independence, as inspectors general do, because of her different constituency. But that belief hinges on institutional culture more than formal legal guarantees. Institutional culture may be too weak a reed to support Privacy Shield, particularly for a court as activist as the CJEU.

In sum, Privacy Shield brings much to the table, including a welcome US candor that will hopefully rub off on our more reticent European allies. The Ombudsperson proposal has significant promise. However, it is too early to tell whether the Ombudsperson can develop a track record of effectiveness that persuades the CJEU and European regulators who found Safe Harbor wanting.

— Peter Margulies

PRIVACY TIP #25

This Week Is National Consumer Protection Week: Know Your Consumer Rights

The Federal Trade Commission (FTC), in collaboration with over 100 governmental, not-for-profit, and private entities, is spearheading National Consumer Protection Week, March 6-12, in an effort to educate consumers about their rights, including information about privacy and identity theft.

The details of the effort are encapsulated in www.NCPW.gov which includes blog posts, articles, resources, and tools for consumers to learn more about consumer issues, including privacy and identity theft. It also provides easy-to-understand information about how to file a consumer complaint with the FTC.

The FTC also recently released its report on consumer complaints, which shows that identity theft continues to be a huge problem in this country.

So celebrate National Consumer Protection Week and learn more about how you can protect yourself and your family with a visit to www.NCPW.gov.

— 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.