Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

September 1, 2016

CYBERSECURITY

FBI Issues a Private Industry Alert for State Election Systems

The Federal Bureau of Investigation (FBI) issued a private industry alert on August 18, 2016, to state Boards of Elections to alert them of hackings into their websites.

According to the FBI, it "received information of an additional IP address, 5.149.249.172, which was detected in the July 2016, compromise of a state's Board of Election Web site. Additionally, in August 2016, attempted intrusion activities into another state's Board of Election system identified the IP address, 185.104.9.39 used in the aforementioned compromise."

The FBI recommends that states "contact their Board of Elections and determine if any similar activity to their logs, both inbound and outbound, has been detected. Attempts should not be made to touch or ping the IP addresses directly."

It further outlines precautionary steps that can be taken, which can be accessed here.

— Linn Foster Freedman

Marine Industry White Paper: Cybersecurity Risks With Voyage Data Recorders

The maritime industry is not immune from cybersecurity risks. Navigation, product supplies and deliveries, radar systems, and GPS systems are all digital and connected in today's world, and can be subject to hacking and intrusions.

Voyage data recorders (VDRs) are connected to essential parts of a ship's navigational and safety systems, including radar, ECDIS, and GPS. Because they are all connected digitally, they can be vulnerable to hacking and intrusions, including the insertion of malware and ransomware into the system, which can disrupt the navigation of the vessel. This result would be devastating to the maritime industry.

Danelec Marine has published a white paper discussing the cybersecurity risks to VDRs and countermeasures that can be taken to make them more secure against risks.

— Linn Foster Freedman

In Wake of Cyber-Attacks, Regulators Focus on SWIFT as Senators Urge Obama to Press G20 to Combat

Cybercrime

As cyber-attacks involving the global payment system SWIFT increase in frequency abroad [see related post], U.S. regulators are discussing steps designed to protect against similar attacks on U.S. financial institutions. The Federal Reserve, Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corp. issued a joint letter last week to Representative Carolyn Maloney (D-NY) of the House Financial Services Community in response to Maloney's inquiries regarding the February theft of millions of dollars from the central bank of Bangladesh.

In the Bangladesh attack, cyber-attackers used stolen operator credentials to submit 35 fraudulent SWIFT transfer requests totaling $951 million. Five of the requests passed, and the criminals made off with $81 million funneled through a web of offshore companies.

In their letter to Maloney, the U.S. regulators said that examiners are now looking more closely at bank links to the SWIFT network and that updated guidance regarding "key controls and risk management practices that should be assessed as part of supervisory oversight" will be issued soon. Maloney responded to the letter with a statement that she is encouraged by the regulators' efforts, but remains "concerned about the potential for future attacks and will be asking for regular updates from our banking regulators."

Also expressing concern over recent SWIFT attacks, six U.S. senators sent a letter to the White House on Monday, urging President Obama to press other nations at the upcoming September Group of 20 Summit to develop a "coordinated strategy to combat cybercrime at critical financial institutions." The senators highlighted the importance of international collaboration, warning that "[our] financial institutions are connected in order to facilitate global commerce, but cyber criminals—whether independent or state-sponsored—imperil this international system in a way few threats have."

— Norman H. Roos and Scott M. Baird

DATA BREACH

Outer Banks Hospital Reports Breach of PHI in Loss of Two Thumb Drives

Everybody knows how much I hate USB and thumb drives. The latest scheme is for hackers to leave thumb drives in coffee shops, airports, office buildings, libraries, and other public places. These USB and thumb drives contain malware and ransomware and can infect an entire system if they are plugged into a home or work computer. So USB drives are *bad,* and unencrypted USB drives are even worse and should be prohibited from use.

But this story, believe it or not, has to do with lost thumb drives containing protected health information (PHI) of an unknown number of patients that were transferred to two unencrypted thumb drives during an acquisition of one hospital by another. During the transaction, the patient data was transferred to two unencrypted thumb drives, which were then lost during transfer.

Unfortunately, the thumb drives contained the PHI of patients for the past 12 years. The PHI included the names, demographic information, emergency contact telephone numbers, patient account numbers, medical record numbers, Social Security numbers, insurance ID numbers, physician names, medical diagnosis, mental health information and medical histories. All this on two unencrypted thumb drives.

— Linn Foster Freedman

Orleans Medical Clinic Notifies 6,890 Patients of Data Breach

Orleans Medical Clinic (Orleans) in Indiana has notified the Office for Civil Rights that the protected health information of 6,890 patients was compromised as a result of an upgrade to its server. Orleans is in the process of notifying the affected patients whose information was exposed. According to Orleans, when it upgraded its server, its electronic health record was unsecured and accessible to hackers for 12 days.

All current and former patients' information, including names, addresses, dates of birth, and Social Security numbers was exposed between April 5, 2016, and April 17, 2016, to hackers.

— Linn Foster Freedman

SCAN Health Plan Notifies Patients of Data Breach Affecting 87,000 Individuals

SCAN Health Plan of California, SCAN Health Plan Arizona, and VillageHealth are in the process of notifying certain plan members and nonplan members of a breach of protected health information, including names, addresses, telephone numbers, dates of birth, and, in some cases, health notes, medications, doctor information, and Social Security numbers.

The unauthorized access to the health plan information occurred between March and June of 2016, when SCAN's sales contact sheets system was compromised. The compromise was discovered on June 27.

Question? Why do sales contact sheets include health information and Social Security numbers? This is another lesson of why it is so important to only ask for and give data that is essential to the purpose of the project. Do sales personnel really need access to individuals' Social Security numbers and why would people give a sales person their Social Security number in the first place?

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

LabMD Seeks Stay of FTC's Final Order Pending Appeal

Not surprisingly, on August 30, 2016, LabMD filed its Application for a Stay of the Final Order of the Federal Trade Commission (FTC), pending review of the order by the appellate court. But, because the matter is still pending before the FTC, the request for the stay had to be filed with the FTC, which recently ruled against LabMD [see related post]. That is an example of a conundrum within administrative law—having to go back to the enforcer to seek a stay of the enforcement action in order to seek a higher authority's review.

It will be interesting to see if the commission will agree to a stay while LabMD continues to fight it over its rejection of the administrative law judge's (ALJ) decision that the FTC's claim that it had jurisdiction over LabMD's data security practices had no merit. The ALJ found that no consumers had suffered harm from the alleged data breach and, therefore, recommended dismissal of the FTC's enforcement action against LabMD. The ALJ also found that the expert reports and testimony submitted by the FTC relied on false testimony and were based on speculation.

This saga continues, and we will be watching closely to see how the FTC reacts to the request for a stay and how the appeal moves forward. We have been following this very interesting case for years, and it

will continue to be a great case study for privacy law students in my class.

— Linn Foster Freedman

Court Declines to Dismiss Jason Pierre-Paul's Suit against ESPN and Adam Schefter

The lawsuit filed by New York Giants defensive end Jason Pierre-Paul against ESPN and ESPN reporter Adam Schefter for invasion of privacy has survived its first challenge from ESPN. We wrote about Pierre-Paul's lawsuit, which arose from a tweet by Schefter that contained a photo of Pierre-Paul's medical records, here.

ESPN filed a motion to dismiss Pierre-Paul's claims in April, asserting that the information tweeted by Schefter was protected by the First Amendment as truthful information related to a matter of public concern. In a ruling issued from the bench, U.S. District Judge Marcia G. Cooke dismissed Pierre-Paul's claim pursuant to Florida Statute § 456.057(7)(a), which provides that medical records "may not be furnished to...any person other than the patient, the patient's legal representative, or other health care practitioners and providers involved in the patient's care or treatment, except upon written authorization from the patient." However, Judge Cooke declined to dismiss Pierre-Paul's claims for invasion of privacy. A written decision is expected from Judge Cooke, which could shed more light on the court's view of ESPN's First Amendment argument.

Judge Cooke's decision on the motion to dismiss may mean that Pierre-Paul's claims are headed for serious settlement discussions, which could include guidelines for tweeting information in the future. For the time being, however, Pierre-Paul's suit has survived the first real challenge from ESPN.

— Kendra L. Berardi

FTC Requests Comments on Safeguards Rule

The Federal Trade Commission (FTC) issued a press release on August 29, 2016, indicating that it is seeking comments on the Standards for Safeguarding Customer Information, applicable to financial institutions.

The Safeguards Rule went into effect in 2003 and requires financial institutions to develop and implement a comprehensive information security program for customer information.

Specifically, the FTC seeks comments on what the economic impact and benefits of the rule, possible conflicts between the rule and other federal or state laws or regulations, and how any technological, economic, or other industry changes may affect the rule.

Comments on the Safeguards Rule can be made until November 7, 2016, and will be posted on the FTC website.

— Linn Foster Freedman

DATA SECURITY

NAIC Released Draft of Revised Insurance Data Security Model Law for Review

The National Association of Insurance Commissioners' (NAIC) Cybersecurity Task Force released a revised draft of the Insurance Data Security Model Law (Model Law) last week. The Model Law's goal is to "establish exclusive standards…for data security and investigation and notification of a data breach" for "any person or entity licensed, authorized to operate, or registered" pursuant to state insurance laws. The Model Law was first released in April of this year and received over 40 comments from trade associations, market participants, and regulators. This week, at the NAIC National Summer Meeting, the Task Force met with interested parties to discuss comments on this new draft. Written comments on the Model Law may be submitted by September 16, 2016.

The revised Model Law addresses the following:

Purpose, Intent, Applicability, and Scope: The Model Law originally preempted state and federal laws addressing data security and breach notification but now states that it is "not to be construed as superseding, altering, or affecting any statute, regulation, order or interruption of law in this state, except to the extent that such statute, regulation, order or interpretation is inconsistent with the provisions of this act and then only to the extent of the inconsistency."

Definition of Consumer Clarified: This includes but is not limited to applicants, policyholders, insureds, beneficiaries, claimants, certificate holders, and others whose personal information is in a licensee's possession, custody or control—regardless of whether a contractual relationship exists.

The Implementation of the Information Security Program: Must be appropriate to the size and complexity of the insurance company.

Risk Management: NIST Framework Dropped: The Model Law originally used the National Institute of Standards and Technology's (NIST) cybersecurity standards; now, removing the reference permits flexibility for insurance companies.

Encryption: The definition changed from "rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security" to "the transformation of data into a form which results in a low probability of assigning meaning without the use of a protective process or key."

Oversight by Board of Directors: This removes the insurance company's board of directors to approve the written information security program; however, the board is still responsible for oversight.

Oversight of Third-Party Service Provider Arrangements: This removes highly restrictive requirements on third-party service provider agreements to "contract only with third party service providers that are capable of maintaining appropriate safeguards for personal information."

Consumer Rights before a Data Breach: Removal of the section regarding consumer notice of the types of personal information collected and stored by the insurance company; the NAICs Insurance Information and Privacy Protection Model Law.

Notification of Data Breach: Insurance companies must notify insurance commissioners within three days of a breach; insurance commissioners also have the final say regarding the notification to consumers. A draft must be sent to the insurance commissioners before consumers will receive notice. The definition of breach and personal information were also revised to limit the scope of what constitutes a data breach.

Consumer Protection Following a Data Breach: This retains the requirement that insurance companies offer identity theft protection services and permits the insurance commissioner to "take other

action deemed necessary to protect consumers."

Private Right of Action: This removes the reference to the creation of a private right of action.

Enforcement Procedure and Penalties: This is a reference to the enacting state's administrative procedure act or insurance code applicable to administrative enforcement proceedings for serious violations.

This new revised Model Law responds to several of the issues raised by commenters but still does not address the effect on overlapping federal and state laws, the timing and content of breach notifications, how insurance companies can comply with obligations under the Model Rule to update their information security program, or the broad authority of insurance commissioners to order consumer protection measures after a data breach. Check out the full revised Model Rule and make sure to submit your comments before September 16.

— Kathryn M. Rattigan

DRONES

Final Drone Rule and Potential Privacy Implications for Operators

Well, the Federal Aviation Administration's (FAA) Part 107 commercial drone regulations are in full swing this week, and without the inclusion of specific privacy standards, there are still concerns about privacy-related drone issues. As we reported last week, the Electronic Information Privacy Center (EPIC) filed a complaint against the FAA alleging that the final drone rule fails to include privacy regulations. For now, until resolution of that claim, commercial drone operators should note a few aspects of the final drone rule that have some sort of privacy implications.

There are three provisions to pay attention to:

1. **No Operation Over People**

   Drones may not be flown over persons unless those persons are directly participating in the drone flight, except when those persons are under a covered structure, inside a covered stationary vehicle, or when the FAA has provided a specific waiver for such operations.

2. **Operation Only in Visual Line of Sight**

   Drones may only be operated in visual line of sight of the drone's visual observer. This means that the drone must be close enough to be seen without the aid of any device (not including corrective lenses of course). This presumably precludes drones from observing distant subjects or places far beyond the operator's line of sight.

3. **No Night Operations**

   Drones may not be operated at night without a special waiver from the FAA. However, operating of drones 30 minutes before official sunrise or 30 minutes after official sunset are permitted as long as the drone is equipped with appropriate anticollision lighting. Drones are essentially prohibited from capturing images under the cover of darkness.

While none of these aspects of the final drone rule specifically address privacy concerns, they are important requirements to know and remember if your company starts to use drones in its day-to-day

operations.

— Kathryn M. Rattigan

PRIVACY TIP #50

FTC Issues Brochure on 10 Ways to Avoid Fraud

With more and more information online, it is easy to accumulate a lot of information about individuals just by using a search engine. Scammers use online information to build profiles of victims and then use different scams to try to defraud victims, particularly the elderly and vulnerable populations. But even the most savvy can become a victim to a sophisticated scheme.

To assist consumers, the FTC issued a brochure today to assist consumers with protecting themselves from fraud. It is not rocket science but a good reminder of ways to protect yourself from the ever-changing landscape of criminals trying to make an easy buck, including through digital means.

Take some time over the long weekend to read the brochure. It is a quick but good reminder of the vigilance we all need to use to protect ourselves from those who are trying to steal our identity and our money every day.

The brochure can be accessed here.

Happy Labor Day weekend!

— 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 relevant areas. The following are several upcoming speaking engagements:

- September 12 - 15 – (ISC)² Security Congress in Orlando, FL (Linn F. Freedman)
- October 11 & 12 – InfoGovCon in Providence, RI (Linn F. Freedman)
- October 24 - 26 – Privacy + Security Forum in Washington, D.C. (Linn F. Freedman)
- November 15 – ABA Webinar: "Assessing the Situation: How to Identify and Evaluate the Cyber and Data Risks that a Contractor Bears" (Linn F. 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

Robinson & Cole LLP