June 23, 2016

CYBERSECURITY

International Maritime Bureau Warns of Cyber-Attacks

Following the issuance of Plymouth University Maritime Cyber Threats Research Group study on the risk of cyber threats [view related post], the International Maritime Bureau (IMB) recently issued a warning to shipping and maritime companies to "be vigilant to the potential commercial impact that cyber-attacks can cause."

In particular, the warning alerted the industry "that emails being sent to and from ships are monitored and altered. This could have a huge commercial effect on vessels."

The International Maritime Organization has approved interim guidelines on maritime cyber risk management which are designed to provide "high-level recommendations for maritime cyber risk management," which will help the maritime industry safeguard the industry "from emerging threats and vulnerabilities related to digitization, integration and automation of processes and systems in shipping." A must read for our clients and friends in the maritime industry.

— Linn Foster Freedman

World Energy Council Warns Utility Industry of Advanced Malware

The World Energy Council recently warned the utility industry that one of the top threats to the energy sector is advanced malware attacks. The warning noted that the utility sector is vulnerable because of the size of the organizations, which lend them to having multiple networks, including industrial control systems, payment systems and customer service systems.

The four types of malware that utility operators should anticipate include:

- Backdoor malware: hackers establish a "backdoor" into the company's network through remote access Trojans (RATs) and botnets and can remain in the system undetected putting the entire system at risk.
- Banking Trojans: malware that is typically used to access bank accounts by stealing login credentials. These Trojans are now being used to steal other types of online credentials, including credentials in the energy sector.
- Ransomware: used to encrypt the victim's data and make it inaccessible until an amount of money (usually in Bitcoin or other virtual currency) is paid. It has been increasing rapidly.

- Wipers: erase your data. It spreads like malware, and can lead to loss of control of the system or disable critical systems if a robust back up system is not in place.

The warning outlines the steps to combat the malware, which includes:

1. Establish the strongest perimeter defense possible.
2. Segmentation.
3. Protect data and key operations through encryption, network monitoring and testing.

— Linn Foster Freedman

First Home Cyber Protection Insurance Offered by Hartford Steam Boiler

The Hartford Steam Boiler Inspection and Insurance Company has announced that it is offering "the first personal lines cyber insurance program for consumers, protecting against computer attacks, cyber extortion, online fraud, and the breach of personal information involving smart homes, computers, and connected home devices."

With the increase in the Internet of Things, the company stated smart home equipment is vulnerable to attack and "until now, there hasn't been a comprehensive cyber insurance policy designed for consumers."

— Linn Foster Freedman

DATA BREACH

Illinois Data Breach Law Amended and Includes New Twists

Illinois Governor Bruce Rauner signed several new provisions into law amending Illinois' Personal Information Privacy Act, including adding health insurance and medical information into the definition of personal information that triggers notification in the event of a data breach.

Health insurance information under the law includes an individual's health insurance policy number or subscriber identification number as well as the content of an individual's application and information provided to a health insurer through a website or mobile application.

The law also includes biometric information as personal information that requires notification, including a fingerprint, and retina and iris images, as well as user names or email addresses in combinations with passwords or answers to security questions.

Interestingly, the new law also requires health care providers to notify the Illinois Attorney General within five days of notifying the Office for Civil Rights of a data breach pursuant to the HIPAA breach notification regulations. This is a first of its kind and is significant since the definition of a breach of security is not the same in the two statutes.

The new law does not recognize a safe harbor if the information was encrypted if the key was or is reasonably believed to have been acquired in the data breach.

Finally, following Massachusetts, Rhode Island and Connecticut, the Illinois law requires all businesses to "implement and maintain reasonable security measures" including adding data security provisions in all contracts when personal information is disclosed to a third party.

This provision emphasizes the continued interest in having regulators which companies are responding to by requiring downstream vendors to protect the data in the same manner as the company, and the importance of vendor management and contractual provisions.

The new law goes into effect on January 1, 2017.

— Linn Foster Freedman

DATA PRIVACY

IRS Makes Exempt Organizations' Form 990 Data Available in Machine-Readable Format

On June 16, 2016, the IRS announced that it will be making Form 990s available in machine-readable format through Amazon Web Services. While this information has always been available to the public, it was previously only accessible in PDF format, making searching or viewing data in bulk nearly impossible. The IRS announcement is in response to a January 2015 ruling by the Northern District of California that the IRS was required, under the Freedom of Information Act, to make Form 990 data available in a machine-readable format. The lawsuit was brought by government transparency group PublicResource.org. (See *Public.Resource.Org v. IRS*, case number 3:13-cv-02789, in the U.S. District Court for the Northern District of California, San Francisco Division).

The vast majority of tax-exempt organizations are required to file a Form 990, which is the IRS's primary tool for gathering information about these organizations. The documents made available will include all Forms 990, 990-EZ (filed by smaller organizations), and 990-PF (filed by private foundations) filed electronically with the IRS from 2011 to the present, as well as related schedules. (Approximately two-thirds of all Form 990s are electronically filed.) Certain donor information, as well as personally identifiable tax identification numbers, will not be released, in order to prevent misuse of the data.

Form 990s include detailed information regarding an organization's finances, board members, executive compensation, fundraising activities, grant-making, and other programs and operations. Making this information available in a searchable and machine-readable format will give the media, charity watchdog groups, researchers and the public easier access to the data, allowing them to identify and track trends across the nonprofit sector, as well as catch inconsistencies in reporting. Similarly, state regulators will be more easily able to identify markers on the Form 990 that may signal potential embezzlement, unreported self-dealing, or other wrongdoing, or that an organization is in financial trouble. This increased transparency may lead to greater scrutiny of their returns, and of the nonprofit sector as a whole.

— Carly Leinheiser

DOJ and DOE Issue Guidance on Privacy Rights of Transgender Students

On May 13, 2016, the Department of Justice and the Department of Education issued a "Dear Colleague Letter" (DCL) describing reasonable steps to protect transgender students under Title IX of the Educational Amendments of 1972 (Title IX) as well as the Family Educational Rights and Privacy Act (FERPA).

Title IX prohibits discrimination on the basis of sex in any federally funded education program or activity, including discrimination based on a student's transgender status. FERPA prohibits a school from disclosing personally identifiable information from a student's education records without consent, unless an exception to FERPA's general consent rule applies. The DCL states that the nonconsensual disclosure of a transgender student's personally identifiable information (PII), including the student's birth name or sex assigned at birth, could be harmful to or invade the privacy of transgender students and may also violate FERPA.

The DCL provided the following guidance regarding the privacy rights of transgender students:

- A student's transgender status may only be disclosed to individual school personnel who have a legitimate educational interest in the information, even if the student voluntarily discloses this information to some members in the school community.
- Generally, schools may disclose "appropriately designated directory information" if the disclosure is not harmful or an invasion of privacy. A student's sex, including transgender status, is not directory information because its disclosure could be harmful or an invasion of privacy.
- Schools may receive requests to correct a student's education records to reflect a student's gender identity and new name. Updating the student's education records "will help protect privacy and ensure personnel consistently use appropriate names and pronouns."

    - Under FERPA, a student has the right to request that inaccurate or misleading information, or information in violation of the student's privacy rights, be amended. If the school decides not to amend a record in accordance with a student's request, the school must inform the student of his or her right to a hearing on the matter. If, as a result of the hearing, the school still decides not to amend the record, the eligible student has the right to insert a statement in the record. The statement must remain with the contested part of the student's record for as long as the record is maintained and be disclosed whenever the record to which the statement relates is disclosed.
    - Under Title IX, a school must respond to a request to amend information related to a student's transgender status consistent with its general practices for amending other student's records. If a student or parent complains about the school's handling of such a request, the school must promptly and equitably resolve the complaint under the school's Title IX grievance procedures.

The DCL was accompanied by a separate document from the Office of Elementary and Secondary Education, *Examples of Policies and Emerging Practices for Supporting Transgender Students*, which provides state and school district policies that address protecting a student's privacy regarding transgender status, ensuring that a transgender student is called by the appropriate name and pronouns, and handling requests to change the name or sex designation on a student's records.

— Kathleen E. Dion

Controversy Looms Over ECPA Amendment in Wake of Orlando Terrorist Attack

After the terrorist attack in Orlando earlier this month, the Electronic Communications Privacy Act or ECPA has been discussed quite a bit. The ECPA, a law which took effect in 1986, limits the government's access to electronic communications and other information. Due to the advancement in technology over the past 30 years, Congress finds itself playing a bit of a balancing act between protecting an individual's privacy and ensuring governmental agencies have the power to enforce laws and protect the public.

The Senate is considering an amendment to the ECPA that would expand the government's ability to collect electronic information through a National Security Letter (NSL). An NSL would allow the FBI to

access customer records held by banks, telephone companies, Internet Service Providers, and others without the need for an order from a judge.

FBI Director James Comey has said the amendment is needed to clear up any confusion about what information the agency can gather without a judge's permission. He says the agency's work has been slowed in "a very, very big and practical way."

Large technology companies including Yahoo, Google, and Facebook, recently wrote to Congress opposing the amendment, saying "the amendment would dramatically expand the ability of the FBI to get sensitive information about users' online activities without court oversight."

Interestingly, Conn Carroll, a communications director for Sen. Mike Lee, noted in an email on June 15 to Law360 that the FBI "found the Orlando shooter twice before he attacked and did nothing, thus there is zero evidence that giving them this additional invasion of privacy would have prevented anything."

The expansion of NSL's is included in the Intelligence Authorization Act for Fiscal Year 2017, as wells as in the amendment to the ECPA reform bill.

— James Merrifield

SOCIAL MEDIA

North Carolina Cyberbullying Statute Struck Down as Unconstitutional

On February 9, 2012, Robert Bishop was arrested and charged with one count of cyberbullying under the North Carolina Cyberbullying statute, which states that it is "unlawful for any person to use a computer or computer network to…[p]ost or encourage others to post on the Internet private, personal, or sexual information pertaining to a minor"..."[w]ith the intent to intimidate or torment a minor."

The case started when high school students posted negative pictures and comments about a male classmate on Facebook, including sexually themed text messages that the male student had inadvertently sent to a male classmate. The situation escalated and numerous posts were added that were sexual, name calling, and insulting.

The student's mother became aware of the situation and called the police. The police used undercover Facebook accounts to view the postings and conduct an investigation. Following the investigation, six students were charged with cyberbullying.

Bishop was convicted and he appealed. He alleged that the statute was unconstitutional under the First and Fourteenth Amendments and punishes protected speech based on its content.

The Supreme Court found that the law restricts speech that is content based, not content neutral, and that the statute's scope was not sufficiently tailored to serve the State's interest in protecting children from the harms resulting from online bullying, and found the statute to be unconstitutional.

— Linn Foster Freedman

DRONES

FAA Releases New Part 107 Regulations for Small Unmanned Aircrafts, Benefit for Commercial Drone Operators

On June 21, the Federal Aviation Administration (FAA) released Part 107 to the FAA regulations regarding commercial operation of small unmanned aircrafts. Part 107 provides operating rules for drone operators who do not fall into Section 336 to operate the aircraft in the national airspace. Part 107 allows for drone operations if the drone is in line of sight, weighs under 55 pounds, hits speeds less than 100 MPH, and flies below 500 feet. Additionally, Part 107 requires that the 'pilot in command' either hold a remote pilot airman certificate or be under the direct supervision of a person who does hold a remote pilot certificate. U.S. Transportation Secretary Anthony Foxx said, "We look forward to working with the aviationcommunity to support innovation, while maintaining our standards as the safest and most complex airspace in the world."

However, the rule does not contain any regulations regarding privacy issues related to the use of drones. The FAA advises drone operators to check local and state laws before collecting information through remote sensing technology or photographs. The rule takes effect in late August of this year. To view the FAA's summary of Part 107 click here.

Part 107 does not apply to model aircrafts. Model aircraft operators must continue to abide by the requirements of Section 336 of Public Law 112-95, which will now be codified in Part 101, including the requirement that they be operated only for hobby or recreational purposes.

— Kathryn M. Rattigan

Embry-Riddle Aeronautical Released Guide for Novice Drone Operators

Everywhere you look there is another news story about drones. Now, Embry-Riddle Aeronautical University's Worldwide Campus has released the first comprehensive consumer guide to buying and using small unmanned aircraft systems (sUAS or drones as they are better known). This new guide can be used by businesses or individual drone enthusiasts who want to learn more about the different types of sUAS that are available on the market and which ones will match up with the operator's skill and experience. The guide also includes information regarding sUAS's performance, quality of construction, ease of operation, cost, accuracy of advertised capacity and user support offerings. Right now, there are approximately 2.5 million sUAS platforms operating in the United States' airspace, with over 7 million sUAS expected by 2020. To read the full guide and brush up on your drone knowledge, click here.

— Kathryn M. Rattigan

PRIVACY TIP #40

Dashcam Apps and Driving Habits

Huh? What is a dashcam app?

A dashcam app uses a smartphone on the dashboard of a car to record traffic accidents, cars running red lights and bad drivers causing accidents. Dashcams can detect hard braking and can automatically record a collision through the use of voice activation. They are also being used to combat insurance fraud. Some insurance companies give discounts for the use of a dashcam so you can prove what a good driver you are.

But what if you aren't such a good driver? A new app, Nexar dashcam smartphone app, is coming out this year that will provide "real-time warnings" and alert drivers using the app to steer clear of bad drivers. This dashcam app records all of the other cars and license plates around you and analyzes and stores the information in basically a bad drivers database. It will also analyze potholes and dangerous intersections and alert the driver using the app of bad drivers, pot holes and dangerous intersections in real time.

The app uses the camera on your phone and records cars speeding past on the right (or left), illegal turns or dangerous maneuvers and stores it for future reference. When that car travels near you on the road in the future, it will alert you so you can steer clear. Others are using dashcam apps that have the ability to register your license plate to associate it with bad driving habits.

Automobile manufacturers' interest has been piqued and it is reported that they are considering automatically incorporating the technology into cars. Looks like your driving habits will no longer be secret—good or bad. Just know that when you cut someone off, instead of receiving a gesture, you may be captured on video.

— *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 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)
- September 12 - 15 – ASIS 2016: 360° VISION in Orlando, FL (Linn F. Freedman)
- October 24 - 26 – Privacy + Security Forum in Washington, D.C. (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.