Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

March 31, 2016

CYBERSECURITY

MedStar Health Newest Health Care Victim of Cyber-Attack

MedStar Health has announced it has shut down its electronic medical record system after confirming that it has been struck with malware.

MedStar indicated that it doesn't yet know whether the virus is ransomware similar to other recent attacks against health care entities but that no protected health information has been compromised. MedStar, which consists of 10 hospitals in the Washington, D.C., area, is staying open and using paper health records.

— Linn Foster Freedman

BigLaw Firms Hit with Cyber Intrusions

Just a week after we reported that the FBI warned international law firms that they are targets for cyber hackings [view related post], multiple (reportedly up to 50) BigLaw firms have confirmed that they have been victims of hackings and intrusions. Further attempts are expected.

The FBI and Department of Justice have reportedly opened an investigation in the Southern District of New York to see if any information was stolen from the law firms. The information could be used in insider trading schemes.

— Linn Foster Freedman

Listen Up White Hats—Uber Is Paying Bug Bounty

Uber recently announced that it has launched a bug bounty program that will pay white hat hackers up to $10,000 for exposure of information that identifies "critical issues," such as Social Security numbers, credit card numbers, bank account numbers, and driver's license images. If the white hat can take over the full account of the rider/partner without interaction, Uber will pay the hacker for the information on how they did it on a sliding scale.

Uber will pay up to $5,000 for the exposure of “significant issues,” which includes “Stored Cross-site Scripting which can cause significant brand damage (e.g., in a homepage), missing authorization checks leading to the exposure of email addresses, date of birth, names, phone numbers, etc.”

“Medium issues” will be rewarded with a payout of $3,000, which includes “access control issues which do not expose PII but affect other accounts…”

As of March 28, Uber had rewarded multiple white hats with payments and had “resolved” many other reports. Uber “thanked” 66 hackers and had closed 99 reports as of this writing.

— Linn Foster Freedman

Car Hackings and Vulnerabilities Update (Jeep/Fiat + GM)

Jeep/Fiat has been sued by a putative class alleging that they were harmed as a result of researchers’ ability to hack into a Jeep and take control of it. Jeep/Fiat filed a motion to dismiss, stating that the owners suffered no harm.

The Jeep/Fiat owners have fired back, stating that they have been harmed because they overpaid for the vehicles that had faulty security, that they never would have purchased the vehicles had they known about the defect, and that the resale demand and value has been diminished because of the revelations. They also argued during a motion to dismiss that the security defect of the vehicles could allow criminals to hack into their cars’ electrical systems. Finally, they also allege that they don’t need to show that the vehicles were actually hacked to be successful in their claims.

Jeep/Fiat alleges that the plaintiffs have suffered no harm and that the suit is based on speculation, and therefore, the case should be dismissed.

On an opposite note, General Motors (GM) got ahead of the curve when it solicited help through a public disclosure program to find out about any vulnerabilities in its cars and is using those reports to learn about and fix any vulnerabilities.

GM invited computer researchers to try to hack its vehicles as part of a bug bounty program, although GM did not pay for any of the information from the hackers. GM will use the information to patch any security issues found through the bug bounty program.

— Linn Foster Freedman

Recent Indictment Underscores Threat to Financial Institutions’ Cybersecurity

In an era of cyberwarfare, financial institutions can find themselves in the crossfire. The U.S. government indicted seven Iranian hackers last week, charging the individuals for their roles in a 2011 series of cyber-attacks targeting at least 46 major banking institutions. The attacks, which attorney general Loretta Lynch called “relentless,” “systematic” and “widespread,” were carried out for nearly a year and included targets such as JPMorgan Chase, Wells Fargo, Bank of America, NASDAQ, and the New York Stock Exchange.

Banks have long known of the danger posed by distributed denial-of-service (DDoS) attacks in which hackers crash a target’s network by flooding it with high levels of traffic. In this case, the Iranian programmers hit some financial institutions with DDoS attacks on a nearly weekly basis, paralyzing bank

infrastructure and locking users out of online banking. Such attacks have been increasing in frequency and sophistication in recent years, with Arbor Networks' recent Worldwide Infrastructure Security Report finding that 57 percent of financial institutions had experienced a DDoS attack, the highest rate of any sector.

Although the indictment falls short of characterizing the attacks as acts officially sanctioned by the Iranian government, intelligence experts have suggested that the campaign was orchestrated as retaliation for the United States' alleged cyberattack on Iran's main nuclear enrichment plant. That attack, revealed in 2010, employed the so-called Stuxnet virus to disrupt Iranian centrifuges used in the enrichment of uranium. Not coincidentally, the recent U.S. indictment also charged the seven Iranians with launching a cyber-attack designed to take control of a small dam in New York.

Commentators remain skeptical that any of the Iranian hackers will ever be brought to trial, but one thing is certain: financial institutions must continue to improve their cybersecurity infrastructure, which may face threats not only from individuals but potentially from foreign governments as well.

The full indictment can be downloaded here.

— Norman H. Roos

ENFORCEMENT + LITIGATION

Class Action Suit Filed Against 21st Century Oncology for Data Breach

We previously reported that 21st Century Oncology had suffered a data breach and notified 2.2 million patients that it had been the victim of a hacking that exposed the names, Social Security numbers, physicians' names, diagnosis information, and insurance information of its patients [view related post].

Although the intrusion occurred in October 2015, 21st Century claimed it was unaware of the breach until the FBI notified it on November 13, at which time 21st Century announced that it had delayed notifying the patients until early March at the request of the FBI as they investigated the intrusion.

Despite the request of law enforcement to delay notification (which is allowed in virtually all state breach notification laws and HIPAA), 21st Century was sued in a putative class action suit in federal court in Florida that alleges that 21st Century violated the Fair Credit Reporting Act and the Florida Deceptive and Unfair Trade Practices Act by failing to detect the intrusion and, further, by withholding the information from the patients. The patients allege that they should have been alerted sooner so they could protect themselves.

We expect that the plaintiffs' claims that 21st Century should not have heeded the FBI's request to delay notification, particularly in view of state law provisions that specifically allow such a delay, will be vigorously defended.

— Linn Foster Freedman

FTC Signs MOU with Canada on Do-Not-Call and Anti-Spam Enforcement Activities

In a sign of increased cross-border cooperation for enforcement purposes, the Federal Trade Commission (FTC) recently signed a Memorandum of Understanding (MOU) with the Canadian Radio-television and Telecommunications Commission that outlines cooperation between the two enforcement

agencies on Do-Not-Call and anti-spam enforcement efforts.

According to FTC Chairwoman Edith Ramirez, the MOU will "enhance cooperation…as we work together to combat illegal telemarketing and spam." It includes joint Do-Not-Call enforcement activities and increased information exchange between the two agencies, which will assist with cross-border enforcement actions.

The MOU requires that the agencies keep the information shared between the two agencies confidential.

— Linn Foster Freedman

Focused Technologies Fined $3.1 Million for Outsourcing to India

Focused Technologies Imaging Services (Focused Technologies) of Menands, New York, was awarded a $3.45 million contract by the state of New York back in 2008 to digitize and scan records of background checks of 22 million people. The information contained in the background checks included fingerprints, Social Security numbers, signatures, dates of birth, and the reasons why the fingerprints were collected. Focused Technologies was specifically tasked with protecting the security of the information and ensuring that a majority of the work be done by individuals with disabilities (also known as a "preferred source" contract with the state). However, Focused Technologies found that it was in fact cheaper to outsource the work to an Indian company for only $82,000, so they contracted with this Indian company to process 16 million individuals' records.

Focused Technologies' plan was discovered by the state, and now the company has agreed to pay $3.1 million in penalties and fees for defrauding the state of New York. Additionally, Focused Technologies must participate in an independent monitoring program for the next five years to make sure that it acts in compliance with future government contracts. Attorney General Eric T. Schneiderman said, "If you are a government contractor and you illegally ship jobs overseas, you will be held accountable." Luckily, after investigation by the state, no evidence was uncovered that indicated the information was redisclosed beyond the outsourcing company in India, and all information has been destroyed. The lesson: beware of outsourcing (and adhere to the terms of your contract).

— Kathryn M. Rattigan

Google Latest Defendant in Biometrics Case

We have been following and reporting on the Facebook and Shutterfly biometrics cases in Illinois and California.

Google was recently sued by a potential class in Illinois alleging that it violated the Illinois Biometric Information Privacy Act by collecting the "faceprints" of individuals without their consent through its Google Photos service, even when they don't have a Google Photos account.

The complaint alleges that, when someone uploads a photo into the service, Google analyzes the photographs by locating and scanning the person's face and extracts geometric data on the contours of the face and creates a template of the face.

We expect that Google will file a motion to dismiss, and we will keep you updated on this third biometrics case filed in Illinois.

— Linn Foster Freedman

Wearable Device Data Discoverable in the Courtroom?

One in five U.S. consumers are tracking their every movement, from their heart rate, skin temperature, and respiratory rate to their activity levels, food intake, weight, and sleep patterns. With this so-called "black box" for the human body, this data collected through our wearable fitness devices has great potential to be used to bolster or dispute a claim related to personal injury, or even any claim where the individual's health information is at issue in the case.

To date, wearable device data has not been used too frequently in the courtroom. In March 2015, in Lancaster, Pennsylvania, this data was used to contradict a defendant's statement that she was sleeping at the time of the crime when in fact the data showed that she was active and awake. In November 2014, in Canada, the plaintiff used her own wearable device data to show that her physical activity had decreased after sustaining an injury in a car accident.

While these uses seem reasonable, there are still many kinks to work out. First, who truly owns the data? The fitness tracker company? The individual? Depending on the privacy policy associated with the wearable device, it all depends. Second, depending on who owns the data, how do you compel disclosure if you need the individual's password and login credentials? This same issue has arisen when counsel seeks to access an individual's social media account. Third, the privacy of the information is sticky. Because wearable fitness device companies do not fall under the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the information may not be considered confidential or protected. Lastly, the relevancy and reliability of the data are highly disputed, not to mention the defenses that could pop up: hearsay objections, inaccuracy or unreliability of the device, authentication concerns, constitutional challenges and just the basic fact of proving whether the individual really wore the device or whether it was a friend or relative instead.

This wearable device data is surely plentiful and could potentially be the smoking gun in many cases. However, discovery concerns still exist. While this data has not been used in many cases thus far, we are sure to see an increase of attempts to introduce this data in the courtroom regardless of these issues.

— Kathryn M. Rattigan

HIPAA

Transfer of Health Care Website Information to Facebook Alleged to Be a HIPAA Violation

Filed under the title of creative lawyering, a putative class action case has been filed against Facebook in federal court in Northern California alleging that health care providers and medical organizations have violated HIPAA by allowing Facebook to access user data from searches on the medical providers' websites.

The plaintiffs allege that when they visit a medical website, like cancer.org, to search for information about a specific type of cancer, the website transfers the user's search to Facebook. They further allege that Facebook then uses the information to sell marketing opportunities to third parties.

While creative, we expect Facebook to move to dismiss the case quickly.

— Linn Foster Freedman

DRONES

Drones Increasingly Used by State Departments of Transportation Across the Country

Across the United States, state Departments of Transportation (DOT) are using or testing drones to conduct bridge inspections, accident assessments, and surveys and to conduct risk mitigation. A recent report by the American Association of State Highway and Transportation Officials found that 17 state DOTs are using drones in these ways, and an additional 16 DOTs are working on drone policies for their state or attempting to get drone research projects started related to infrastructure inspections. The two states with the most drone-active DOTs are Michigan and Minnesota.

Back in 2014, the Michigan DOT worked with the Michigan Tech Research Institute to conduct a study on the viability of drones and found that drones "provided a mechanism to keep [their] workers out of harm's way" from the risks associated with "setting up work zones, detouring traffic and using heavy equipment." Instead, the study found that drones "can get in and get out quickly, captur[e] data in near real-time and caus[e] less distraction and inconvenience to drivers." Additionally, the study determined that a manual inspection of a freeway bridge takes eight hours, four workers, and costs about $4,600 whereas a drone can do the job with two people in two hours for only $250. You do the math. Minnesota conducted a similar study through the state as well.

The lesson? Drones should be (and are likely to become) a better option for many of the everyday tasks conducted by DOT workers. Drones can improve the quality of freeway bridge inspections and certainly lower the costs associated with those inspections. And surely drones can be used outside the state DOT context; businesses can look to drones to increase operational safety and lower costs associated with many mundane tasks.

— Kathryn M. Rattigan

FAA 2016 to 2036 Aerospace Forecast Released

Last week, the Federal Aviation Administration (FAA) released its "*2016 to 2036 Aerospace Forecast,*" stating that "there is optimism that the industry has been transformed from that of a boom-to-bust cycle to one of sustainable profits." According to the report, profits will not be the only thing hitting the skies; the FAA predicts dramatic increases in the number of drones hitting the airspace. The FAA estimates the use of small, hobbyist drones will grow from 1.9 million in 2016 to almost 4.3 million by 2020, while the use of drones for commercial purposes will grow from 600,000 in 2016 to 2.7 million by 2020. This forecast is based on the "improved regulatory environment and underlying demand," says the report. The report also includes some statistics on the registered drones under the new FAA Rule issued earlier this year. As of March 2016, there have been over 408,000 registrations for small drones under 55 pounds. In the commercial realm, as of March 16, 2016, the FAA has issued over 4,000 Section 333 exemptions for commercial drone operations. Both of those numbers are sure to increase.

Paired with this increase, the FAA reports that it will continue its education and outreach through its "Know Before You Fly" educational campaign. Additionally, the FAA reports that it has partnered with test site operators and educational institutes to focus on research, education, and training for safe integration of drones into our airspace. Check out the full report for more details and information on aerospace across the country.

— Kathryn M. Rattigan

FAA Increases Altitude for Commercial Drones

On March 29, 2016, the Federal Aviation Administration (FAA) announced that its "blanket" altitude authorization for Section 333 exemption for commercial drone operators will increase from 200 feet to 400 feet. After an extensive risk evaluation, the FAA determined that commercial drones can fly up to 400 feet except in restricted airspace. FAA Administrator Michael Huerta said, "Expanding the authorized airspace for these operations means government and industry can carry out unmanned aircraft missions more quickly with less red tape." However, all commercial drone operators must still comply with other existing rules such as only flying the drones in daylight, within the visual line of sight, and at least five miles from a control tower of an airport. This is yet another step in the right direction for businesses looking to utilize drones to cut costs and increase efficiency.

— Kathryn M. Rattigan

McElroy Films Secure FAA Section 333 Exemption

Boston video production company McElroy Films, LLC (McElroy Films) recently secured its Federal Aviation Administration (FAA) Section 33 exemption, adding its name (and services) to the list of 22 other commercial drone operators in the state of Massachusetts. The owner of McElroy Films, Ben McElroy, said, "We have been able to capture incredible footage through drone based cinematography–visually arresting aerials that were previously unachievable without helicopters, flight plans, permits…a lot of red tape, and all coming at a much greater expense to the client. Not only is drone videography much safer and cost effective for our clients, but honestly, it's a great deal of fun and clients are always extremely impressed with the results."

As of March 16, 2016, the FAA has issued over 4,000 Section 333 exemptions for commercial drone operations. Of course, McElroy Films will need to follow specific guidelines for flying its drones to capture video and image, including the use of only specific drones (e.g., the DJI Phantom 2); only use the drones for aerial videography and photography for corporate, education, nonprofit, surveying, and real estate; and be operated by an individual with a sport or recreational pilot's license (as well as a FAA airman medical certificate or U.S. driver's license) and an observer must be in constant communication and sight of the drone to ensure safe operation. While this was a two-year task for McElroy Films to secure its Section 333 exemption, many other companies are currently applying for this exemption as well and more are sure to join the trend.

— Kathryn M. Rattigan

PRIVACY TIP #28

What Do You Do If You Are a Victim of IRS Tax Fraud?

It's tax season. The dreaded April 15 federal tax filing deadline is looming. You try to be diligent, and you file your tax return early, hoping to get an early refund. But when you try to e-file your return, it gets rejected because you have already submitted your tax return and your refund has already been processed. But you didn't file and you for sure never got your refund. What happened? You have become another one of the 700,000 Americans who have become the victim of tax fraud.

According to the IRS, “tax related identity theft is when someone uses your Social Security number to file a false tax return claiming a fraudulent refund.” Your tax account is most at risk if your wages and Social Security number were affected by a data breach.

With all of the phishing schemes, data breaches, and cyber intrusions happening, tax fraud is only expected to rise.

What do you do?

Here are some tips:

1. File a complaint with the FTC advising that you have become a victim of identity theft.
2. Got to IRS.gov and review the materials posted on what to do and follow the instructions.
3. Complete IRS Form 14039, which is an affidavit that certifies that you are a victim of identity theft.
4. Yes, you still have to file your real tax return, but you can do so in paper. Include the affidavit when you send in your paper tax return to the IRS.
5. Respond to any written correspondence from the IRS. Please note that the IRS never calls or contacts taxpayers over the telephone, so if you get a call purporting to be from the IRS, do not respond or give any information to the caller—it is just another fraudster with another scam.
6. For special assistance, call 1-800-908-4490.

Happy tax season. May you e-file without any issues. And if you are getting one, enjoy that refund.

— 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.