Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

September 15, 2016

CYBERSECURITY

Hackers Post Athletes' Medical and Drug Testing Records Online

Hacking group Fancy Bear, reportedly a Russian group who allegedly hacked into the Democratic National Committee emails, which made headlines, has posted U.S. Olympians' medical and drug testing records online. Although it has been described as a "smear" campaign, the U.S. Olympians, in Olympian style, tweeted and thumbed their noses at the hackers, saying that the records show that they did everything by the book.

The World Anti-Doping Agency (WADA) announced that the hackers were previously linked to the Russian government, but the hackers disputed that claim and said they were associated with Anonymous.

At any rate, the effect was minimal. WADA said in response to the hacking, "In fact, in each of the situations, the athlete has done everything right in adhering to the global rules for obtaining permission to use a needed medication. The respective International Federations, through the proper process, granted the permission and it was recognized by the IOC [International Olympic Committee] and the USADA…The cyber-bullying of innocent athletes being engaged by these hackers is cowardly and despicable."

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

Former IRS Employee Reports to Prison for Identity Theft and Fraud

Nakeisha Hall was sentenced in federal district court in August to serve nine years and two months in prison after she pleaded guilty for crimes she committed while working for the IRS Taxpayer Advocate Service. Instead of advocating for taxpayers, she actually used taxpayers' personal information to commit fraud and identity theft against them.

Her job was to help taxpayers who were victims of identity theft, but in fact, she used their information in a tax fraud scheme with three others that netted them $1.5 million after filing false tax returns. She stole taxpayers' identities through unauthorized access to IRS computers and then filed the false tax returns.

She reported to prison on September 13, 2016. In sentencing her, the judge stated, "This is one of the most extensive tax fraud schemes I've ever seen." The judge also commented that, although she was entrusted to help taxpayers who had already been victims of fraud, "Instead you preyed on them and victimized them again."

After serving her prison sentence, she will then undergo five years of supervised release.

— Linn Foster Freedman

Cruise Line to Pay up to $76 Million to Settle TCPA Violations

Caribbean Cruise Line Inc., The Berkley Group, Inc., and Vacation Ownership Marketing Tours, Inc., settled a Telephone Consumer Protection Act (TCPA) class action last week for up to $76 million (and not less than $56 million). The three were sued for violating the TCPA by robocalling millions of individuals with offers for free trips. The plaintiffs in this class action included one million individuals who received calls from Caribbean Cruise Line and its subsidiary marketing companies between August 2011 and August 2012. Those individuals are expected to receive about $500 per call received as a result of this settlement. The exact amount of consumer awards will be determined once the exact number of individual claims is determined. Those individuals who appear on the list of one million consumers will be allowed to receive their award, and those individuals who are not on the list but make a claim will need to prove that they received a call within that time frame. Again, another lesson to know TCPA requirements and make sure that your company is sticking to them.

— Kathryn M. Rattigan

DATA PRIVACY

Start-up Joberate Assigns Score to Employees to Determine Their Job Search History

Most individuals seeking new job opportunities use their personal email address to correspond with a prospective employer, presumably keeping that job hunt secret from their current employer. Now, however, Joberate, a start-up that tracks an individual's job search activity in public social media accounts, calculates a score of how likely each individual is looking for a job. Joberate scours publicly available data from millions of individuals' online social media accounts (or buys the information from other parties) to assign each individual what Joberate calls a "J-Score" that estimates their level of job search activity. For example, if an individual starts following new companies on Twitter, clicking through articles about resume writing or career-related content on their Facebook feed, or making a series of professional connections on LinkedIn, the J-Score goes up. Joberate then shares these scores with their clients for purposes of keeping tabs on talented outsiders or to see how engaged their own workers are at their own jobs. Joberate does not see activity that is set to private, and it does not pick up on general online searches. However, if you use an "Apply with LinkedIn" button on a job posting or you comment on a story about job searches that uses Facebook to collect comments, Joberate could detect the activity and include it in the individual's J-Score. The J-Score takes into account an individual's typical social media use and job responsibilities to create a baseline score. This type of predictive analytics is being used more and more by many different sectors. For now, it is unclear how valuable companies will find this data to be, but Joberate's client base is certainly on the rise.

— Kathryn M. Rattigan

DATA SECURITY

Hardware Password Defaults – Do You Change Them?

IT professionals have long understood the importance of changing the default password for network-connected hardware devices (printers, switches, wireless access points, etc.). In the world of the Internet of Things, it seems everything is connected to the Internet: the locks to your house, your refrigerator, your car, the wireless router from the cable company, and the list goes on. All of these devices have a default user name and password for managing settings. IT professionals should know better than to ever leave those administrator passwords as a default, but does the general public?

In September 2015, the InfoSec Institute published a detailed article regarding the exploitation of corporate printers (InfoSec Institute). In January 2016, several news outlets reported on hackers using the storage in network-connected printers and multifunction devices to store and execute malicious code (*SecurityWeek*). In March, it was reported how hackers printed anti-Semitic flyers to thousands of publically accessible printers (*Washington Post*). As recently as Friday, September 9, Security Week

reported on a new malware variant, Mal/Miner-C, discovered by Sophos, that specifically targets network-attached storage devices, leveraging default user name and passwords (*SecurityWeek*).

Whether you are an IT professional or a home consumer, hackers continue to exploit vulnerabilities in other network connected-devices besides your traditional computer. Based on the recent discovery of Mal/Miner-C, hackers continue to see the default user name and password as a way into those devices. Clearly, we are not doing a good enough job at adhering to what amounts to age-old advice: *change the default administrator password immediately and disable any unused or unnecessary services*. If you don't plan to have your refrigerator order your groceries for you, turn that service off and be sure to change the default password on that fancy new garage door lifter.

— Sean Lawless

Three Golden Rules for Managing Third-Party Security Risk

Vendors that have access to company data continue to be a high risk when it comes to data security.

Check out this article I wrote that was published in *Information Week Dark Reading* to get tips on how to manage security risks with third parties: 3 Golden Rules For Managing Third-Party Security Risk

— Linn Foster Freedman

DRONES

New Tool for Companies Seeking Qualified Drone Pilots

As more and more drones enter the skies, more and more companies are seeking qualified drone pilots to operate Unmanned Aircraft Systems (UAS) for their business. Skyward, a drone operations management platform, has now released "Pilot Finder," an easy way for companies to find qualified UAS pilots who also meet certain job requirements. Pilot Finder's database includes information on each operator, including:

Areas of expertise and services provided

- Total and historical flight hours;
- Qualifications, licenses, exemption, and certificates (e.g., Federal Aviation Administration Part 107 Remote Pilot Certificate or sport's license); and
- Insurance coverage and service area.

Pilot Finder can be used for a one-time flight or to hire a flight tester for a drone manufacturer. Skyward CEO Jonathan Evans says, "Skyward supports commercial operations for companies at every stage and size, and our goal is to always help our clients eliminate inefficiencies and headaches." The new Pilot Finder will help to connect companies with qualified drone pilots and simplify the process of running a drone operation. Check out more about Pilot Finder here.

— Kathryn M. Rattigan

Is There a Way to Monetize Commercial Drone Data?

By the end of the year, it is estimated that there will be about 600,000 commercial drones operating in the United States. U.S. Transportation Secretary Anthony Foxx says, "We are in one of the most dramatic periods of change in the history of transportation." From agricultural to infrastructural surveying to package delivery and even firefighter drones, drone use is on the rise. But the new question that the drone industry is asking is this: how do we make money using commercial drones' data? Consider that on average a drone captures ten megabyte still frame images or video each second during a flight. That is a

lot of raw data. Most of the time, these megabytes of data are processed using photogrammetry (i.e., the use of photography in surveying and mapping to measure distances between objects) applications, or the individual pixels are analyzed to find patterns or anomalies. Monetization of that data occurs once the captured raw data is processed into a finished data product. Only at that point can the expense of commercial drone operations and their flights generate revenue. DroneData, a Texas-based drone application company, is working on figuring out that number. For now, drone flights will continue to increase along with the vast amount of new data we will collect from each of those flights.

— Kathryn M. Rattigan

PRIVACY TIPS

Privacy Tip #52 – Sharing Your Information with Your Rental Car

Those of you who know me (and my husband and children will attest) know that I will not ask for directions. I am definitely more like a man than a woman when it comes to refusing to stop and ask for directions.

But I also refused to download Waze ever since it required that you basically give up your entire contacts list to them, and I don't like to put my location-based services on for Google maps. So what's a stubborn girl to do when I am in a foreign city trying to get to my destination?

Most rental cars now give you the option for GPS (and as soon as you turn the car on, it says, "Welcome, Linn Freedman") and the ability to connect your cell phone to the blue tooth feature in the car. So the last time I rented a car, I looked at that GPS screen that knew who the driver was, and I knew that they were also tracking everywhere I drove. And when the screen said to connect my cell phone to the blue tooth, I knew that it was tracking every telephone call I made, down to the exact number I called. Is that something that the rental car agency really needed to have? What would they do with that information? So, obviously, I didn't use the GPS, nor did I connect my phone.

Apparently, I wasn't the only one concerned. Soon after my case of paranoia, the FTC issued a consumer alert about sharing data with your rental car. According to the FTC, precautions that rental car customers can take to ensure the safety of their information when driving connected cars include:

- Drivers should avoid connecting their phones or electronic devices to an infotainment system for the sole purpose of charging. If your phone is low on battery, it's better to use a cigarette lighter adapter to charge instead of the USB port, which may automatically transfer and store data. (Geez, I didn't even catch that.)
- If you do connect a device to the infotainment system, it may display a screen to ask which types of information you want the system to know. In this case, be sure to only grant access to necessary information; for example, don't share your contacts if you only want the system to play music.
- Delete all personal data from the infotainment system before returning the vehicle. Within the system's settings, you should be able to locate a list of devices connected with the system and follow instructions to delete data. If the process proves tricky, the car's manual or rental company should be able to give more information.

The FTC warning states that if drivers don't delete this data before the car is returned, they risk the possibility of sharing it with future renters, rental car employees, or cybercriminals.

Just be aware of these facts and make an educated decision on what information you want to leave behind after you return that rental.

— 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:

- 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.