Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

October 29, 2015

CYBERSECURITY

Senate Passes Cybersecurity Information Sharing Act

After a long delay, with a vote of 74 to 21, the United States Senate passed the Cybersecurity Information Sharing Act (CISA) on October 27, 2015.

The bill has been touted as being controversial and is opposed by privacy advocates, some tech companies and several Senate Republicans as it "would grant legal immunity to companies who in sharing information actually violate your privacy."

On the other hand, the U.S Chamber of Commerce and dozens of business entities and groups support the bill, which gives companies a safe harbor from liability if they share cybersecurity incidents and cyber intrusion information with each other and the government. The bill paves the way for companies and the government to share critical information that will assist in combating cyber attacks against U.S. companies and the government.

The measure now moves to the House for reconciliation before it can hit President Obama's desk for signature. It is nice to see both sides of the Senate working together to pass crucial cybersecurity legislation.

— Linn Foster Freedman

NIST Seeks Comments on Guide to Help Financial Sector Manage IT Assets

The National Cybersecurity Center of Excellence is seeking comments on a draft practice guide, entitled *IT Asset Management* (Special Publication 1800-5a) which is “designed to help the financial services industry monitor and manage IT hardware and software assets more securely and efficiently.”

The guide helps companies bring separate data systems used for physical assets, security systems and IT into a single system so they can identify and better manage the organization’s risk.

The guide can be downloaded from NCCoE’s website.

— Linn Foster Freedman

NIST Seeks Comments on Privacy-Enhanced Identity Brokers Project Document

The National Cybersecurity Center of Excellence, in partnership with the National Strategy for Trusted Identities in Cyberspace National Program Office, have launched a project designed to imbed privacy and security measures into identity broker solutions.

What is an identity broker? It is a third-party service provider that companies use to manage its multiple third-party credentialing options. This means that individuals can use logins across sites and be authenticated. So you can use your Facebook login credentials to access your account with a Facebook partner, such as Amazon.

It is pretty difficult for companies to manage all of these login credentials, which is where identity brokers come in. They manage those credentials options for companies.

The project will "examine how commercially available privacy-enhancing technologies can be integrated into identity broker solutions." The document, called "Privacy-Enhanced Identity Brokers," describes the "technical challenges faced when attempting to add privacy-enhancing technologies to existing products or services, and the technical controls needed to address the privacy risks inherent in them."

The comments generated will be used to develop an example solution and a practice guide.

Comments can be given via a web form from the NCCoE website or by email to petid-nccoe@nist.gov.

— Linn Foster Freedman

Hacker Arrests and Prosecutions Update

We previously reported that alleged Ukranian hacker Sergey Vovnenko, also known as "Flycracker," "Fly" and "Darklife" was extradited from Italy, arrested and charged in New Jersey federal court for his part in disbursing the nasty malware Zeus on October 13.

During his arraignment last week, he pled not guilty to charges, including wire fraud conspiracy, unauthorized computer access and aggravated identity theft. He is being detained without bail.

Another hacker from Kosovo, who is well known to law enforcement, 20-year-old Ardit Ferizi, known as "Th3Dir3ctorY," has been arrested in Malaysia.

Ferizi is alleged to have stolen the data of 1,351 U.S. military and government personnel, which he then turned around and gave to a member of the Islamic State group, who then posted a 30-page document on Twitter that contained the demographic and location information of the individuals. The Twitter message stated, "NEW: U.S. Military AND Government HACKED by the Islamic State Hacking Division!"

Ferizi was arrested when he travelled to Malaysia to study computer science at a private university. Sounds like he would have gotten an easy A in that course.

The U.S is seeking extradition of Ferizi for prosecution. If found guilty, he faces up to 35 years in jail.

Kudos to the DOJ for its continued progress in bringing these hackers to justice.

— Linn Foster Freedman

DATA PRIVACY

EU Safe Harbor Update

Last week, the Vienna Higher Regional Court ruled that most of Max Schrems' claims against Facebook can proceed, including his claim that Facebook improperly allowed his personal information to be shared with the National Security Agency. So his case can move forward, but the court did not allow him to represent other claimants in a class action type lawsuit, as Austria does not recognize class action lawsuits. However, he was given the right to appeal that issue as it is one of first impression, which he publicly stated he would do.

The German data privacy commissioner has issued a press release stating that, as a consequence to the European Court of Justice's (EJC) verdict, the federal commissioner should "leverage existing opportunities to strengthen data protection for European citizens in a sustainable way."

The commissioner, Andrea Voßhoff, stated that she expects a clear signal from the European Commission in response to the ruling of the ECJ and progress in the negotiations with the United States. She welcomed the period granted by the Art 29 Working Party until the end of January 2016.

She also urged the U.S. to take this chance to substantially improve protection of fundamental rights to European citizens for data transfers from Europe to the United States and commented that the Judicial Redress Bill, which has passed in the U.S. House of Representatives, is a first step while further commenting that it is not sufficient in its current version.

Finally, the privacy commissioner stated that affected companies need to be aware that data transfers solely on the basis of safe harbor are immediately unlawful until the end of January 2016 and clarification is required on legal issues and the consequences of other existing methods for data transfer to third countries such as Binding Corporate Rules and EU model clauses.

— Linn Foster Freedman

Google Mandates Full Disk Encryption

With the release of Android 6.0, code name Marshmallow, Google has mandated that OEMs (Original Equipment Manufacturers) enable full disk encryption. Google is requiring that the feature be enabled as part of the "out of box experience" for customers setting up new mobile devices. Google previously attempted to do the same for Android 5.0, code name Lollipop but, due to performance issues on some manufacturer's devices, eased their requirement. Regarding Android 6.0, even if the customer skips setting the secure lockscreen, the device will encrypt using a default PIN.

Apple has mandated partial or full disk encryption since iOS version 8. Because it seems like everyone has an iPhone anyway, why should Google's revitalized push for mandatory encryption matter? Because, in actuality Apple only holds approximately 42 percent of the U.S. market share. Worldwide that drops to a surprising low of approximately 14 percent. So while it may seem that everyone you know has an iPhone, the data tells us that when we look at the greater pool of mobile device users most of them are using Android.

Google's recent announcement is a huge step forward in mobile data privacy & security.

Related Articles:

- Google Pushes Mandatory Full-Disk Encryption In Android 6.0
- Android 6.0 Will Finally Require Manufacturers To Enable Full Disk Encryption By Default On New Devices
- Smartphone OS Market Share, 2015 Q2
- comScore Reports March 2015 US Smartphone Subscriber Market Share

— Sean Lawless

New "Tracker of Terms and Conditions" Service Released, Tracks All the Changes, All the Time, to a Website's Terms of Use

We have all read a website's terms of use (hopefully), and almost all of the terms say something to the effect of "these terms may change without prior notice, so we recommend that you review them regularly." Well now, an organization has released a new tracker called "Tracker of Terms and Conditions" that runs comparisons every 12 hours of over 5,600 services and 6,700 sets of terms to track the changes, list the changes (and date of the changes), and supply a color-coded list of the changes based on the significance of the change. In addition to access to this list, consumers can also subscribe to Tracker of Terms and Conditions' website and receive notice when specific companies revise their terms. New services like this suggest that perhaps consumers are starting to care a bit more about what companies say in their terms of use. The lesson: be transparent, be concise, and inform your users when a material change is made.

— Kathryn M. Rattigan

ENFORCEMENT+LITIGATION

Uber Class Action Case Hits Roadblock

A California federal judge has ruled that a former Uber driver who is suing Uber in a proposed class action case was unable to show that he suffered an immediate threat of identity theft and dismissed the driver's first amended complaint.

The driver alleges that Uber failed to keep his personal information, and that of 50,000 other Uber drivers, safe and the information was hacked and released in a data breach in March of 2014. The information accessed included drivers' names and license numbers. The plaintiff alleged that the information was used to open a Capital One credit card.

The judge balked and said that "It is not plausible that a person could apply for a credit card without a Social Security Number."

This case continues the long line of cases that hold that a plaintiff in a data breach case is unable to show standing to sue if there is no imminent or immediate threat of harm.

— Linn Foster Freedman

Court "Likes" NLRB's Determination that Facebook Posts Are Protected under the NLRA

The Second Circuit Court of Appeals recently upheld the National Labor Relations Board's (NLRB) decision that employees' Facebook posts are protected by the National Labor Relations Act (NLRA). *Three D, LLC d/b/a Triple Play Sports Bar and Grille v. National Labor Relations Board.* The case involved two employees and a former employee engaged in a Facebook discussion regarding their employer's alleged improper tax withholdings. A former employee posted this: "Maybe someone should do the owners of Triple Play a favor and buy it from them. They can't even do the tax paperwork correctly!!! Now I OWE money…[expletive]!!!!" A second employee "liked" that comment while a third employee commented: "I owe too. Such an [expletive]."

The Court upheld the NLRB's determination that the one employee's "like" and the other employee's comment were protected under the NLRA and that the employer improperly terminated the two current employees. Under the NLRA, employees have the right to engage in concerted activities for the purpose of mutual aid and protection, and employers are prohibited from interfering, restraining, or coercing employees in the exercise of that right. Because the Facebook posts were made among current employees in the context of workplace complaints about tax liabilities, tax withholding calculations, and claimed owed back wages, the Court affirmed the NLRB's conclusion that the employees were engaged in concerted, protected activity.

While employers have a legitimate interest in protecting their reputation and services or products from disparagement and harm, the Court agreed with the NLRB that the employees' posts were not sufficiently disloyal or defamatory to lose protection under the NLRA. Specifically, no evidence existed that the statements were made with knowledge of their falsity or reckless disregard of whether they were true or false. Nor did the statements refer to the employer's products or services or otherwise disparage the employer.

Finally, responding to the employer's argument that the Facebook posts contained obscenities that could be seen by customers, the Court responded, "Almost all Facebook posts by employees have at least some potential to be viewed by customers. Although customers happened to see the Facebook discussion at issue in this case, the discussion was not directed toward customers and did not reflect the employer's brand. The Board's decision that the Facebook activity at issue here did not lose the protection of the Act simply because it contained obscenities viewed by customers accords with the reality of modern-day social media use."

In light of the Court's decision, before disciplining or discharging employees for their social media use, employers may choose to consider whether the comments are protected under the NLRA.

— Peter A. Dagostine

HIPAA

Arrest of Immigrant at Texas Clinic Isn't a HIPAA Issue

Immigration advocates have alleged that a Texas clinic violated health care privacy laws by calling the police when a woman gave a fake driver's license as authentication to receive medical services. But if the clinic provided services to someone who was clearly not using proper identification, it could be aiding the commission of medical identity theft. View the article published in Law360.

— Linn Foster Freedman

Privacy Tip #7 — Who Is Listening to Your Conversations through Your Smartphone Microphone?

I've always known that my smartphone had a microphone. If nothing else, it obviously has to be used for the Shazam app so I can figure out the name of that great song. So that is the only time I use the microphone on my phone. And then when I am finished using the Shazam app, I turn it off. You'll see why if you read on.

Most people have no idea that there even is a microphone setting on their phone, let alone the amount of data that goes through the microphone on smartphones if it is on all the time.

I first became interested in the capabilities of smartphone microphones after I spoke with a security expert who was employed with a defense contractor. He told me that he never enables his microphone on his phone and even if it isn't enabled, he never keeps his phone on at all while he is working at his desk at the defense contractor. I said "Why--if it is off?" He raised his eyebrows and said, "Linn, really? Of course there is technology that can enable a microphone even if you don't...turn off your phone when you are working at your desk or any time your phone is near you and you aren't using it." Hmmm. He didn't seem like he was trying to spook me. I did more research and got sufficiently spooked.

So practically speaking, what are the privacy issues with the microphone setting on your phone?

It is accessible. It is hackable. If you use Sirius or any other apps that use your microphone, you are allowing that app to have access to anything that can be heard with it on. Someone can listen to everything going through your microphone when your phone is on if the microphone is on. Think about how Shazam works. It can actually listen to the music that is playing in the restaurant and identity it for you. It can also hear everything else around you--your conversations with your spouse, with your children, with co-workers and literally everyone else you come into contact with.

You don't care that all of your conversations can be heard? That's ok That's your choice.

But make an educated choice. If you do care, go to settings on your phone, click on microphone and see which apps have requested and you have agreed to use your microphone. Turn off that capability if you don't want that app to have access to all of your conversations. In many instances, when you download an app, it automatically includes permission to use the microphone when you click "I agree." Also, turn your microphone off and only turn it on for apps that need it for specific purposes that you allow (like Shazam) or don't allow it at all.

Whatever you do, make an educated choice and know who you are allowing to use the microphone feature on your phone and limit access and use where you feel appropriate.

— 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.

Boston | Hartford | New York | Providence | Stamford | Albany | Los Angeles | Miami | New London | rc.com