
**August 6, 2015**

# Data Privacy + Security Insider

---

**DATA SECURITY**

**Be Aware of Windows 10 Free Upgrade Opt Outs**

Since July 15, Windows 7 and Windows 8 users have been offered a free upgrade to Windows 10. Windows 10 includes Wi-Fi Sense, which features a default prompt that asks users to share access to WiFi networks that they have connected to with any of their contacts in Outlook and Skype, and an opt-in prompt for Facebook friends.

What does this mean? Every time you join a WiFi network, you will be asked if you want to share your WiFi password with your contacts, friends and social networks so they can join the network too. If you say yes (as many people do automatically when a pop-up comes up on their phone without reading it), the encrypted password is sent to all of your contacts and social networks so they can connect to your network as well.

It is important to read all pop-up messages before you click "I agree," and to read and know what you are agreeing to.

If you don't mind that every single person in your Outlook contacts, Skype contacts and Facebook friends have access to your WiFi network, then clicking "I agree" is right for you. But if you are more concerned about protecting your information, and you don't want this default setting on your phone, security experts are recommending the following:

- before you upgrade to Windows 10, change the WiFi network name to include the terms "_nomap_optout"
- after you upgrade, disable WiFi Sense sharing in privacy settings
- upgrade the security of your WiFi network

Whether you want to use this feature or not, be aware of it, and read all pop-ups and make your own decision each time. They are designed to educate you on how companies are using and sharing your data.

*— Linn Foster Freedman*

## Android Smartphones Stagefright Engine Vulnerable

It is being reported that 95% of all Android smartphones are vulnerable to being hacked with a text message, which is being called the “heartbleed for mobile.” According to security experts, the vulnerability exploits the “stagefright” engine at the core of the Android system and allows the attacker to virtually take over the victim’s device, including the recording of audio and video, access to photos and other data on the phone, and hijacking the Bluetooth capabilities.

Apparently there is no official released patch to date, but security experts advise that you should disable the Hangouts and Messenger apps on your Android. The result: you will not receive text messages until the updated security measures are installed on your phone.

*— Linn Foster Freedman*

---

**INFORMATION GOVERNANCE**

## The Key to Information Governance Success Lies Within the Framework

There is no secret sauce to achieving information governance nirvana. The reality is someone must take ownership of an organization’s information governance program. The industry as a whole has been discussing that organizations appoint a chief information governance officer (CIGO) or its equivalent, to lead information governance efforts. The title is not important—the skill-set is.

If your organization appoints a CIGO, the CIGO can’t drive the information governance program on his or her own. Stakeholder groups from Legal, Compliance, Records Management, Privacy, Security, IT and other business units must be willing to get their hands dirty and get involved. It’s truly a team effort.

After the team has been assembled and roles have been defined, it is essential to list out how the roles of each member of the team work together. No doubt, stakeholders from Records Management, Legal and Compliance will focus primarily on taxonomy and metadata, while IT, and Privacy and Security will focus heavily on infrastructure and technology.

Next, the information lifecycle of a document must be defined from creation to disposition. This is the nucleus of any information governance program. No matter if the document is shared, stored, retained for discovery purposes or disposed of, it’s imperative that governance rules and permissions are applied at every point of the document’s lifecycle.

In line with the information lifecycle, is the execution of technology. This will include the many applications, hardware, networks, service-level agreements and licensing that makes the magic come to life.

Last, but certainly not least, is focusing on the various policies and procedures which define the information governance program. These policies and procedures may define metrics, processes, roles, standards and performance, all with a common denominator of accountability and decision rights.

As mentioned, the creation of an information governance framework is by no means an easy task. It will take much time and effort to align your strategy with the business goal and objectives to ensure the highest level of impact, but it is imperative to a company’s risk management program.

If you would like to discuss information governance, please contact any of the team members here at R+C.

*— James Merrifield*

---

**DATA PRIVACY**

**Will the EU's 'Right to be Forgotten' Law Become Global? Google Sure Hopes Not**

While Google did in fact comply with the Court of Justice of the European Union's (CJEU) May 2014 order, which allowed individuals in Europe to request that a search engine 'delist' certain information about them from Internet links that harm their privacy, and did process over 25 million individual requests for information removal from all European versions of Google Search, the company is not ready to apply this standard globally. This 'right to be forgotten' law applies not only to defamatory or untrue information, but also to news stories, court records, and other lawful materials, as well as accurate, publicly available information.

On July 30, 2015, Google rejected an order by France's data protection regulator that required Google to apply Europe's 'right to be forgotten' law on a global scale. Google said that France's order was a "troubling development that risks serious chilling effects on the Web." Essentially, if Google were to follow France's order, that would mean that an approved removal request by an individual in France, would not only remove the information from google.fr and other European versions of Google Search, but from all versions of Google Search around the world.

To date, Google has received about 55,400 requests from individuals in France since the 'right to be forgotten' law was first announced, and it has already removed almost 75,000 Internet links from its European Google Search domain.

Google said in a public statement, "While the right to be forgotten may now be the law in Europe, it is not the law globally. Moreover, there are innumerable examples around the world where content that is declared illegal under the laws of one country, would be deemed legal in others: Thailand criminalizes some speech that is critical of its King, Turkey criminalizes some speech that is critical of Ataturk, and Russia outlaws some speech that is deemed to be 'gay propaganda.'… [and] [i]n the end, the Internet would only be as free as the world's least free place." Google stated that "as a matter of principle" it respectfully disagrees with France's order and has requested that France withdraw its Formal Notice. We will keep you updated on the outcome of Google's non-compliance and how this might affect the 'right to be forgotten' across the globe.

*— Kathryn M. Rattigan*

---

**ENFORCEMENT+LITIGATION**

**Proposed Class Action Case Filed Against Medical Informatics Engineering**

Medical Informatics Engineering, Inc., an electronic medical record service provider, recently disclosed a data breach affecting approximately 4 million individuals. Within days of the disclosure, Medical Informatics was hit with a proposed class action lawsuit alleging that it should be held to a higher standard as its business is based on data security and it failed to prevent the breach. The suit alleges that the

information stolen included Social Security numbers and medical information.

The case further complained that Medical Informatics delayed to notify the affected individuals.

This week, in response to the disclosure of Medical Informatics, Indiana Attorney General Greg Zoeller advised all citizens in the State of Indiana to activate a credit freeze on their accounts through the three credit bureaus. According to Zoeller, the breach, which included 11 healthcare providers and 44 radiology centers, was one of the largest affecting Indiana residents this year, (up to 1.5 million) and therefore, he is urging Hoosiers to pro-actively protect themselves. Good advice.

*— Linn Foster Freedman*

---

**Neiman Marcus Files Petition for Rehearing En Banc**

We previously reported on the Seventh Circuit's reversal of the District Court's dismissal of the data breach class action case against Neiman Marcus.

On August 3, 2015, Neiman Marcus filed a Petition for Rehearing requesting that the full Seventh Circuit consider the case.

The basis for the Petition is that the Seventh Circuit's opinion was contrary to the U.S. Supreme Court's opinion in *Clapper v. Amnesty Int'l USA* as the plaintiffs were unable to show imminent or certainly impending harm from the data breach.

The Petition further argues that the Seventh Circuit's decision created a split in Circuits, as the opinion is at odds with *Reilly v. Ceridian Corp.*, which held that an increased risk of identity theft from a data breach is insufficient to satisfy standing requirements.

*— Linn Foster Freedman*

---

**Warrantless Access to Cell Phone Location Data May be Heard by the Supreme Court**

A number of courts have considered whether the Fourth Amendment requires the government to obtain a warrant to access historical and/or real time cell phone geographic location information, known as CSLI. CSLI is cell site location data your cell phone gives off when you place or receive a call. Additionally, cell phones also automatically generate location data by continually identifying themselves to the closest cell tower even when there is no live call, and some experts say, even if the cell phone is powered off.

Law enforcement views CSLI as vital to locate and track suspects as part of an criminal investigation, and often seeks the information by filing an application with the relevant court simply stating that the information to be obtained is relevant to an ongoing investigation. The applications may or may not include facts establishing probable cause or even distinguish between location information in either historical or real time. Some court orders granting access do not distinguish between historical or real time data.

Court decisions have been divided on whether probable cause and a warrant is required to obtain CSLI. Last week, a United States District Judge in the United States District Court for the Northern District of California, San Jose division affirmed the judge magistrate's ruling denying the government's application for CSLI on the grounds that a warrant was required to obtain such information. Also earlier

this year, the Florida Supreme Court, in *Tracey v. State of Florida*, held that real time cell site location information is protected by the Fourth Amendment.

However, in May of this year, in *United States v. Davis*, the Eleventh Circuit Court of Appeals reversed an earlier three judge panel upon rehearing en banc, and held there is no reasonable expectation of privacy in these cell phone location records and, even if there were such an expectation, a warrantless search would still be reasonable. 785 F.3d 498.

On July 31, Davis' lawyers petitioned the U.S. Supreme Court to review and overturn the Eleventh Circuit's decision in *Davis v. United States*. If the Court accepts the case, perhaps the Court will resolve the issue of whether the warrant requirement of the Fourth Amendment applies to searches of CSLI.

*— Kathleen M. Porter*

---

**4th Circuit Holds that Obtaining Cellphone Location Information Without a Warrant is Unconstitutional**

We have been watching the warrantless search cases closely. Yesterday, (August 5, 2015), the Fourth Circuit Court of Appeals held that it was unconstitutional when law enforcement used their cell phone location information without a warrant.

Two defendants were convicted of armed robbery. Some of the evidence presented at their trial included location information from their cell phones. The government obtained the information through a court order, as opposed to a warrant. They appealed the conviction saying the government should not have used the information without a warrant, that the search was a violation of their Fourth Amendment rights, and that the court order was insufficient.

Although the Court held that obtaining the location information without a warrant was unconstitutional, it agreed with the lower Court's decision to allow the evidence in the case because the government relied in good faith on the court orders that were issued to obtain the information.

*— Linn Foster Freedman*

---

**FTC Refunds Consumers for Telemarketing Scam**

The FTC recently announced that it is sending more than $969,000 to 10,387 customers who were bilked out of their funds through a telemarketing scam operated by Innovative Wealth Builders (IWB).

According to the FTC, IWB "falsely promised consumers it could reduce their credit card interest rates and save them thousands of dollars on their debts." The FTC sued IWB and alleged that it made false claims to consumers and billed consumers without their consent.

*— Linn Foster Freedman*

---

**HIPAA**

**HHS Issues Fact Sheet on HIPAA Rules and Resources**

The Department of Health and Human Services (HHS) has released a fact sheet on the privacy, security, and breach notification rules of the Health Insurance Portability and Accountability Act (HIPAA). Designed to apply to HIPAA-covered entities, including health care organizations, health care plans, providers, and their business associates, the fact sheet provides a basic overview of the HIPAA rules, the information protected by the rules, and a summary of who is required to comply with the rules. Among other things, the fact sheet includes a table of the breach notification timelines, a chart regarding the different types of covered entities, and a topic index with links to additional resources.

*— Jean E. Tomasco*

---

**DRONE PRIVACY**

**First Meeting of Drone Privacy Stakeholders; Will it Result in any Privacy Guidelines?**

In a previous post, we discussed the Federal Aviation Administration's (FAA) proposed drone regulations, and now, on August 3, 2015, the first drone privacy stakeholder meeting ensued in Washington, D.C., led by the National Telecommunications and Information Administration (NTIA). NTIA director, John Verdi, told media that the goal of this first meeting was to develop working methods, set their priorities, and decide upon the structure of the meetings moving forward.

The NTIA Deputy Assistant Secretary, Angela Simpson, said that the NTIA's underlying goal is to help stakeholders prepare a set of guidelines for drone use, *but not* impose the guidelines on drone users. Simpson said, "We are not regulators. We are not developing rules or brining enforcement actions."

So if the NTIA is not going to enforce any kind of drone privacy regulations who is? Well, a Department of Transportation (DOT) representative told the media that neither the FAA or the DOT has any statutory oversight of privacy. This means that neither the FAA or the DOT will be enforcing the best practices that are established by these drone privacy stakeholders. Essentially, any best practices that stem from these meetings will be used as a "guide" only. With the increased use of drone technology on many fronts, the potential for privacy violations will also increase. For now, the tentative drone privacy stakeholder meetings scheduled for the rest of this year are on September 24th, October 21st, and November 20th. We will keep you posted on any news that comes from this group.

*— Kathryn M. Rattigan*

---

**SOCIAL MEDIA**

**FTC's Social Media Product Endorsement Guidelines**

Back in 2009, the Federal Trade Commission (FTC) updated its 'Endorsement Guides' and followed up with an informal publication called "What People are Asking" to clarify some of the guides points. In May 2015, the FTC updated its guides once again in the FTC's Endorsement Guides: What People are Asking and some new answers to frequently asked questions (FAQs). The basics regarding endorsements are:

1. "Endorsements must be truthful and not misleading."

2. "If there's a connection between an endorser and the marketer of the product that would affect

how people evaluate the endorsement, disclose it clearly and conspicuously."

3. "If the advertiser doesn't have proof that an endorser's experience represents what consumers will achieve by using the product, clearly and conspicuously disclose the generally expected results in those circumstances."

This expanded guide from May 2015, has resulted in some recent questions from social media outlets. For example, one of the updates to the guide and the FAQs discusses the question, "What about a platform like Twitter? How can I make a disclosure when my message is limited to 140 characters?" The FTC says that it "isn't mandating the specific wording of disclosures. However, the same general principle – that people get the information they need to evaluate sponsored statements – applies across the board, regardless of the advertising medium. The words "Sponsored" and "Promotion" use only 9 characters. "Paid ad" only uses 7 characters. Starting a tweet with "Ad:" or "#ad" – which takes only 3 characters – would likely be effective." #FTC guidelines.

And the FAQs also include, "I am an avid social media user who often gets rewards for participating in online campaigns on behalf of brands. Is it OK for me to click a "like" button, pin a picture, or share a link to show that I'm a fan of a particular business, product, website or service as part of a paid campaign?," to which the FTC responds, "Using these features to endorse a company's products or services as part of a sponsored brand campaign *probably* requires a disclosure." Thanks for clarifying. Social media outlets are hoping to get even more updates to these vague guidelines as advertising and endorsements through social media become even more prevalent.

Most importantly, businesses should be sure to include information relating to the credibility of the speaker in all types of advertisements and stay up-to-date on FTC endorsement guidelines.

*— Kathryn M. Rattigan*

---

**CYBERSECURITY**

**2015 US State of Cybercrime Survey Released**

The 2015 US State of Cybercrime survey has been released and is worth a read. The Survey, co-sponsored by PwC, CSO, the CERT Division of the Software Engineering Institute at Carnegie Mellon University and the United States Secret Service is the result of survey responses from more than 500 US businesses, law enforcement services and government agencies, as well as PwC's 18th Annual Global CEO Survey. The goal of the survey is to "provide a more thorough and balanced look into the current state of cybersecurity and cyberthreats."

The basic conclusions are:

- It's been a "watershed year" for cybercrime and cause headaches for business executives
- 76% of the respondents are more concerned about cyberthreats this year (87% of CEOs said they were worried about cyberthreats in PwC's CEO Survey)
- There is a "significant correlation" between company size and the ability to detect incidents
- The most frequently detected compromise is from external actors, and phishing campaigns are on the rise (31% said they had experienced a phishing attack in 2014)
- Cyberattacks are becoming more frequent and destructive, and Distributed denial of service (DDoS) are more potent and frequent
- Ransomware "is becoming more sophisticated and commonplace"
- 50% of Boards view cybersecurity as an IT issue rather than an enterprise-wide risk issue

- Boards are concerned, but not engaged as the CISO or CSO only rarely presents to the Board
- Security executives should proactively engage the Board on cybersecurity risks
- There is “an underwhelming level of participation” in industry-specific Information Sharing and Analysis Centers
- Companies are relying on technology solutions to manage cybersecurity risks
- Vendor and third party risks are just being addressed and regulators in the financial services industry are focusing on due diligence over down-stream vendors (but 1 in 5 C-Suiters say they are not concerned about third party cybersecurity risks)

The conclusions and suggestions in the Survey are sound and easy to understand and should be summer reading for all business executives.

*— 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

---