Attorney Advertising

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

"KRACK" Wi-Fi Security Vulnerability Discovered

Security researchers this week have found a new vulnerability that affects Wi-Fi Protected Access II, also known as WPA2, which is the security protocol used by many wireless networks. The vulnerability, Key Reinstallation AttaCK (KRACK), allows intruders to breach into WPA2 and steal the data being transmitted between a wireless device and a Wi-Fi network, including passwords, messages, and photos. According to the researchers, the vulnerability is also able to inject malware and ransomware into websites and can manipulate data.

Wi-Fi hardware vendors have produced security updates, which companies would do well to follow. To find out whether your hardware vendor is vulnerable, visit the Computer Emergency Readiness Team (US-CERT) website, which lists the at-risk hardware vendors and the patches and advisories for companies to follow. *Read more*

ENFORCEMENT + LITIGATION

Supreme Court to Hear Microsoft Emails Case

In an order issued on October 16, 2017, the U.S. Supreme Court granted certiorari in *United States v. Microsoft Corporation*, a case with potentially far-reaching implications for the privacy of electronic data maintained by technology companies across the globe.

The case, which Robinson+Cole has previously discussed here, here, and here, arises from a warrant obtained by the Department of Justice (DOJ) under the Stored Communications Act (SCA). [1] The SCA was enacted in 1986 to protect the privacy of electronic communications, including by extending privacy protections to electronic records analogous to those afforded under the Fourth Amendment to the U.S. Constitution. [2] In relevant part, the SCA requires a governmental entity in most instances to secure a warrant in accordance with the Federal Rules of Criminal Procedure to compel disclosure of electronic communications stored by a service provider. [3] *Read more*

October 19, 2017

FEATURED AUTHORS:

Wystan M. Ackerman
Pamela H. Del Negro
Conor O. Duffy
Linn Foster Freedman
Kathleen M. Porter
Kathryn M. Rattigan
Matthew P. Rizzini

FEATURED TOPICS:

Cybersecurity
Data Breach
Drones
Enforcement + Litigation
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

Stored Communications Act Does Not Prohibit Disclosure of Deceased's Yahoo Account

In what appears to be a case of first impression in the Commonwealth of Massachusetts, the Supreme Judicial Court (SJC) has ruled that Yahoo may disclose the contents of Yahoo email accounts to their personal representatives and is not precluded from doing so by the Stored Communications Act (SCA). *Read more*

Airline Cargo Company Sued under Illinois Biometric Law

Alliance Ground International is the latest company to be sued for allegedly violating the Illinois Biometric Information Privacy Act (BIPA) for collecting and storing its employees' fingerprints without their consent. The proposed class of employees alleges that the company, which takes employees' fingerprints as part of its timekeeping records for their work as bag handlers at Chicago O'Hare International Airport, is storing their fingerprints without their consent.

BIPA requires businesses that collect biometric data to obtain written consent before using it and to notify consumers about how the data will be used. The proposed plaintiffs allege that, in violation of BIPA, the company never informed the employees of its policies for retaining and using their fingerprints. They are seeking $1,000 per violation or actual damages, whichever is higher, and requesting that the company implement a plan to destroy the data, which is required by BIPA. *Read more*

DATA BREACH

Hyatt Data Breach Impacts 41 Locations in 11 Countries

Hyatt Hotels Corporation recently announced that it had identified a malicious software code resulting in unauthorized access to customer payment card information. Hyatt disclosed that, upon investigating the incident, it discovered unauthorized access to customer payment cards manually entered or swiped at the front desk of 41 Hyatt-managed locations in 11 countries between March 18, 2017, and July 2, 2017. A list of the affected locations and contact information for questions is available here. Hyatt states that cardholder names, card numbers, expiration dates and internal verification codes were affected, but it has no indication that other information was involved. This is the second Hyatt breach in the past two years. The previous incident (described here) involved credit card data at 250 locations in approximately 50 countries. *Read more*

DRONES

Amazon's Scanning Technology for Package Delivery

If you haven't yet heard about it, Amazon is on the forefront of package delivery. And if you think that is old news (which it is!), have you heard about Amazon's scanning technology that is capable of scanning the homes below its delivery drone so it can properly deliver that awesome new gadget you just purchased? Well, what Amazon's patent application stated was that this scanning technology would not only scan the properties below to detect the correct geographical drop location for the package but would also be collected data. *Read more*

Drone Collides with Commercial Jet in Quebec City

On October 12, 2017, a drone collided with a commercial aircraft while approaching Jean Lesage International Airport in Quebec City. This is the first time a drone has hit a commercial plane in Canada, according to Transport Canada Minister Marc Garneau. He stated, "I am extremely relieved that the aircraft only sustained minor damage and was able to land safely." No injuries to the eight passengers on board the airplane were reported. According to Garneau, the accident could have been much worse if the drone had hit the cockpit or engine. *Read more*

PRIVACY TIP #110

Resources for Small Businesses to Stay Informed about Cyber Threats

The Federal Trade Commission (FTC) has concentrated on small businesses this year with the launch of www.FTC.gov/SmallBusiness, which provides data security awareness information to small businesses. The site includes articles about data security, how to develop a data security plan, what happens when ransomware affects your business, and what to do in response to a data breach and offers information relating to the most recent threats affecting businesses across the nation. It also frequently publishes scam alerts, which are helpful to small businesses.

All of the FTC resources are relevant and helpful to small businesses, which will help them to start thinking about data security and addressing the risks posed to business.

In addition to the FTC site, are other resources and websites that provide important information to help small businesses stay abreast of cyber threats and intrusions, including the following:

- US-CERT, which provides industry warnings and information on security incidents, intrusions, and threats that businesses

experience
- IRS website
- National Institute for Standards and Technology (NIST)
- FBI
- InfraGuard
- Specific industry blogs, newsletters or alerts
- Krebs On Security
- www.dataprivacyandsecurityinsider.com

As we approach the second half of Cybersecurity Awareness Month, ask someone in your organization to research several resources that may be helpful to your business. Have that person sign up for relevant alerts, blogs, and newsletters; be a point person for staying informed of cyber threats that may affect your business; keep executives informed of those threats. We have found that each day time must be devoted to keeping up with cyber threats. Having someone devoted to the task is key to staying on top of them.