Attorney Advertising

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

IoT Security Risks Widespread

According to bloggers on techtarget.com, security risks around the internet of things (IoT) continue to be problematic, and a new free guide, "The Developer's Guide to IoT" has been published specifically for IoT device developers, which is a welcome contribution to the industry.

The guide walks developers through ways "to meet the security, analytics and testing requirements for IoT applications." This is important because in the past, developers would develop new IoT products (like refrigerators, security systems, toys, personal assistants), devices, and applications without a clear strategy on how those applications and products would interconnect with other IoT applications and how that interconnectivity could be damaging to consumers. *Read more*

New York Financial Services Cybersecurity Regulations Deadline Looming This Week

On March 1, 2018, the one year transition period within which banks, insurance companies, and other financial services institutions and licensees regulated by the New York Department of Financial Services ("Covered Entities") must have implemented a cybersecurity program ends. By today, the Covered Entities must be in compliance with the following requirements: *Read more*

DRONES

Drones Helping to Restore Power in Puerto Rico

In the mountains near Ponce, Puerto Rico, after Hurricane Maria tore through, the terrain made it difficult to repair power lines that stretched from peak to peak. For over four months, the entire area was in the dark and so were its residents. In January, utility companies started using a new approach to restoring power: drones. *Read more*

Kansas State Offers UAS Training for First Responders

March 1, 2018

FEATURED AUTHORS:

Linn Foster Freedman
Kathryn M. Rattigan
Carrie C. Turner

FEATURED TOPICS:

Cybersecurity
Drones
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

Kansas State University Polytechnic Campus began working with law enforcement partners in the area to offer a training course specifically targeted for first responders seeking to use unmanned aircraft systems (UAS or drones) for daily operations and safety procedures. *Read more*

Drones and Personal Privacy

Imagine that you are sitting in your backyard and a drone flies overhead. It hovers. The camera adjusts and looks right at you. Then it flies away. You are left wondering who is operating it and why. On a number of occasions, similar encounters with unknown drones have led to visceral (sometimes even violent) reactions from the person being observed. *Read more*

PRIVACY TIP #128

Basic Smartphone Settings to Thwart Hackers

When talking to colleagues and friends, it appears that folks do not understand how their smartphones work and the data that can be accessed through them. This prompted me to again give basic steps that can be used to protect personal information that can be accessed, legitimately and in an unauthorized manner, through the settings on their smartphones.

1. Implement the longest passcode possible (not just four digits) and set the passcode to pop up in the least amount of time. Use a passcode that is difficult to guess—that means, don't use 12345 or your birthdate.
2. Eliminate the ability to sign in to applications or websites through a social media account. By signing up through a social media account, that company and every other company that it shares your information with across platforms is tracking you, collecting your data, accessing your information and selling it. More importantly, if one of those social media accounts is hacked, all of them are compromised.
3. Disable auto-connect to public wifi. Do not use public wifi unless you are using a VPN or other secure connection to access sensitive data. Hackers are able to get access to unsecure public wifi sites, and your information can be compromised.
4. Turn off location based services when not using the app. In Privacy Settings, keep location based services off when not using the app and frequently look to see which apps have requested access to location based services. In addition, turn off the location tracking when using social media sites or other websites.
5. Limit access to your microphone and camera. If you have your microphone and camera on at all times, all of the apps that you have given access to the microphone and camera have access to conversations and everywhere you are at all times, whether you are using the app or not. Hackers are able to hack into the apps that you have allowed access to your camera and microphone. These can be adjusted in your Privacy settings on your phone. Frequently check these

settings and which apps you have given permission to use them, and turn them on only while using the app.

6. Adjust privacy settings on social media accounts, including frequently clearing the permissions settings. Remove apps and sites that you do not use so they stop collecting your data.

Frequently checking the privacy settings on your social media accounts and your smartphone is good cyber hygiene and doing so will surprise you at how many apps are, and have been, collecting your data. Securing your smartphone and being cautious about public wifi are basic measures you can put in place to protect yourself from compromise.