Attorney Advertising

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Cyber-attacks are the Third Greatest Global Risk in 2018

A new report issued by the World Economic Forum (WEF) called "Global Risks Report 2018," lists the threat of cyber-warfare and cyber-attacks affecting the public as the world's third greatest threat in 2018, only behind natural disasters and extreme weather.

The report notes that because of an increased global reliance on connected devices and the internet, and the fact that cyber-attacks have doubled over the past five years, the risk will continue to rise in 2018. It cited the WannaCry ransomware attack in 2017, which affected 300,000 computers throughout 150 countries, and NotPetya, which caused business losses in excess of $300 million. *Read more*

NIST Issues Blockchain Technology Report to Help Businesses "Make Good Decisions" About Using Blockchain

On January 24, 2018, the National Institute of Standards and Technology (NIST) issued its "Draft NIST Interagency Report 8202 Blockchain Technology Overview" which it announced as NIST's "Report on Blockchain Technology Aims to Go Beyond the Hype." The press release announcing the issuance of the report starts by stating "Beguiling, baffling or both—that's blockchain. Aiming to clarify the subject for the benefit of companies and other organizations,…NIST has released a straightforward introduction to blockchain," which underpins Bitcoin and other digital currencies…The NIST report's authors hope it will be useful to businesses that want to make clear-eyed decisions about whether blockchain would be an asset to their products. *Read more*

Google Tracking of Android Users Goes Beyond the Expected

By now most smartphone users are aware of location tracking used by both Apple and Android operating systems. Basic location tracking is a system which uses GPS data to know the phone user's location. However, according to a recent article published by *Quartz*, Google's data collection goes far beyond basic location tracking. Not only does

January 25, 2018

FEATURED AUTHORS:

Linn Foster Freedman
Sean Lawless
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Drones
Enforcement + Litigation
GDPR
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

the data collected go beyond simple location information, but the 'opt in' service Google uses to collect that data, Location History, isn't as truly opt in as users might expect. According to *Quartz*, Google's Location History underlies many of Android's main apps, including Google Assistant and Google Maps. Furthermore, opting in to Location History for one app may actually give many apps access to Location History's data and the ability to send that data to Google. What types of data, beyond basic location, are being sent to Google? *Read more*

ENFORCEMENT + LITIGATION

New Class Action Against FAA

The Federal Aviation Administration (FAA) was served with an 836,796-person lawsuit last week alleging wrongful collection of personal data and money under unmanned aerial system (UAS or drone) regulations. This lawsuit, *Robert Taylor v. FAA*, is the second class action filed against the FAA. The first, filed in 2015 by Robert Taylor's brother, John, alleged that applying Part 48 of the FAA UAS regulations to model aircraft was illegal, specifically, the requirement that model aircraft must register with the FAA. Last May, a federal appeals court found that the regulations were indeed illegal, vacating model aircraft registration requirements. However, this December, with President Trump's passage of the National Defense Authorization Act, the ruling was effectively rescinded. *Read more*

GDPR

European Commission Releases GDPR Guidance

All privacy professionals, whether in the EU or the US, need to have an understanding of the implications of General Data Privacy Regulation (GDPR) compliance, particularly since the fines and penalties that could be imposed for non-compliance are intimidating. GDPR goes into effect on May 25, 2018, and many companies are struggling to become compliant by the deadline. The European Commission (Commission) has acknowledged that companies are grappling with how to comply with the daunting new requirements. In response to what has been described as widespread panic, the Commission has released a new website that provides extensive guidance on GDPR implementation, for which we are all grateful. *Read more*

DRONES

Protecting Your Business—Drones and Liability

Unmanned aerial systems (UAS or drones) are getting better (and cheaper) each day, which means that more and more businesses will be using drones to carry out everyday tasks. However, with respect to compliance and risk-management, when businesses hire third-party drone service providers, questions will surely arise regarding liability. Businesses that hire third-party drone service providers will need to carefully review those third-party service providers' compliance with those regulations. *Read more*

First Drone Rescue at Sea

Just last week, the first ever drone rescue at sea occurred in the heavy riptides off the coast of Australia. Two swimmers were trapped in the strong current when a drone dropped a flotation device down to them from the sky. The fate of the two swimmers could have been much worse if it weren't for the drone's ability to quickly and safely get the flotation device into the water. The "Mini-Ripper LifeSAVER" drone was launched by the Coast Guard immediately upon learning of the swimmers' distress. *Read more*

New Jersey Passes Penalty Bill for Prohibited Drone Operations

Last week, New Jersey's state assembly passed legislation, Assembly Bill 520 ("the Bill"), that provides for fines and prison terms for individuals convicted of unsafe and/or prohibited unmanned aerial systems (UAS or drone) operations. Specifically, the Bill will provide for up to six months in jail and fines of up to $1,000 for a conviction for operating a drone in a manner that could endanger life or property, while under the influence of alcohol or drugs, or for the purposes of taking or assisting in the taking of wildlife. For a conviction related to the operation of a drone near a correctional facility, in a manner that interferes with first responders or lawful hunters, or in a manner to circumvent a restraining order, the operator could face between 18 months and five years in prison and fines up to $15,000. Lastly, the Bill allows owners and operators of critical infrastructure (or political subdivisions thereof) to prohibit operation of drones in close proximity to their systems or structures pursuant to the Federal Aviation Administration's (FAA) Extension, Safety and Security Act of 2016. Importantly, the Bill also preempts any municipal or county measure in conflict with these prohibitions or penalties. *Read more*

Farmers Use Drones to Check Their Crops

As a farmer, you likely need to keep a close eye on the growth of your crops or survey hundreds of acres of crops after a storm or other natural disaster. Agriculture experts now say that farmers should look

to the skies for some help in doing so. John Perry, president of the Coastal Plains chapter of the Association for Unmanned Vehicle Systems International (AUVSI), says “Drones have gotten very popular recently, and it’s not just under the Christmas tree. It’s out in the construction, infrastructure, civil engineering, and transportation, but one of the biggest places we’re seeing this technology applied is down on the farm.” Technology, known as precision agriculture, gives farmers a new way to inspect crops, look for damage, detect nitrogen levels, and apply spray applications of fertilizer or pesticides more efficiently. *Read more*

PRIVACY TIP #123

Tax Identity Theft Awareness Week

Who knew—but yes, next week is Tax Identity Theft Awareness Week. How sad is it that we have to have a week devoted to education and awareness on this topic?

It’s tax season (“busy season” as my CPA friends call it), and prime time for identity thieves to reap millions in fake and fraudulent tax returns as they have done in the past.

To combat this widespread and serious problem, the Federal Trade Commission (FTC) has dubbed the week of January 29 to February 2, 2018 as “Tax Identity Theft Awareness Week,” and has announced a number of free webinars, Twitter chats and helpful information to prevent tax identity theft, and resources in the unfortunate event you become a victim of tax identity theft.

The FTC resources can be accessed here.

Here is a schedule of events so far:

January 29 (2 p.m. EST) — The FTC and the Identity Theft Resource Center co-host a webinar for consumers about tax identity theft, IRS imposter scams, how to protect yourself, and recovery steps for victims.

January 30 (2:30 p.m. EST) — The FTC, AARP Fraud Watch Network, AARP Foundation Tax-Aide program, and the Treasury Inspector General for Tax Administration invite consumers to a webinar about tax identity theft and IRS imposter scams.

J**anuary 31** (11 a.m. EST) — The FTC and the Department of Veterans Affairs co-host a Twitter chat for service members, veterans, and their families about minimizing your risk of tax identity theft and recovering if you’re a victim.

January 31 (1 p.m. EST) — The FTC, the Department of Veterans Affairs, and the Treasury Inspector General for Tax Administration discuss tax identity theft, IRS imposter scams, and what to do if you become a victim. This is a closed webinar for Veterans Administration employees, patients, and contractors.

February 1 (1 p.m. EST) — The FTC and IRS offer a free webinar for small businesses about tax identity theft, imposter scams that target businesses, cybersecurity, data breaches, and free resources for your business, employees and customers.

February 1 (3 p.m. EST) — The FTC and the Identity Theft Resource Center invite consumers to join a Twitter chat about tax identity theft, its warning signs, and what to do if it happens to you.

In addition, the FTC has published these tips to fight tax identity theft:

- File your tax return early in the tax season, if you can.
- Use a secure internet connection if you file electronically, or mail your tax return directly from the post office.
- Respond to all mail from the IRS as soon as possible.
- If tax identity theft happens to you, visit IdentityTheft.gov to report it to the FTC, file an Identity Theft Affidavit with the IRS electronically, and get a personal recovery plan.

We all have to file our tax returns, but following these tips may protect you from tax identity theft while you do so.