Attorney Advertising

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

US-CERT Warns of New Ransomware: Bad Rabbit

The U.S. Computer Emergency Readiness Team (US-CERT) is warning companies in the U.S. about a new ransomware dubbed "Bad Rabbit." US-CERT stated it has received multiple reports of infections by Bad Rabbit in countries around the world.

According to security researchers, Bad Rabbit poses as an Adobe update, and when the user clicks on the update, ransomware infects the computer, locks it down, and demands payment of a ransom to retrieve the files. The virus is similar to the two previous ransomware viruses, WannaCry and NotPetya, that attacked companies throughout the world earlier this year. *Read more*

DATA BREACH

Hilton Settles Data Breach Investigations with NY and VT AGs

Hilton Domestic Operating Co., Inc. (Hilton) has agreed to pay the New York and Vermont attorneys general $700,000 to settle allegations it violated those states' consumer protection and data breach notification laws when it failed to implement reasonable security measures to protect consumer data and waited nine months to notify consumers of a data breach. *Read more*

HEALTH INFORMATION

CMS Addresses Lingering Uncertainties and Raises Others via MACRA Information Blocking Guidance

The Centers for Medicare & Medicaid Services (CMS) recently issued guidance intended to help clinicians eligible for the Merit-based Incentive Payment System (MIPS) navigate an attestation required concerning the prevention of information blocking. MIPS was implemented via CMS's Quality Payments Program final rule released in 2016 and represents one avenue for payment reform under the

November 2, 2017

FEATURED AUTHORS:

Conor O. Duffy
Linn Foster Freedman
Kathryn M. Rattigan
Matthew W. Rizzini

FEATURED TOPICS:

Cybersecurity
Data Breach
Drones
Enforcement + Litigation
Health Information
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

Medicare Access and CHIP Reauthorization Act of 2015 (MACRA). Health industry stakeholders, and providers in particular, have repeatedly cited difficulty in communicating between electronic health record systems as a major impediment to effective health care reform (including due to so-called "information blocking" practices). In response, MIPS seeks to incentivize clinicians to promote the interoperability and compatibility of certified electronic health record technology (CEHRT). *Read more*

ENFORCEMENT + LITIGATION

Hyatt and Bob Evans Face Class Action Biometric Suit over Fingerprints

Hyatt Corp. was hit with a class action suit this week for allegedly violating the Illinois Biometric Information Privacy Act (BIPA) by collecting and storing employees' fingerprints. This is the latest in a string of suits over the same complaint—employers using employees' fingerprints for time clock systems without their written consent.

The named plaintiff alleges that she has to clock in and out of work using a fingerprint scanner. She alleges that Hyatt never obtained her written consent to collect her fingerprint, which is a violation of BIPA, nor did it inform her of how her fingerprints would be used, how they would be stored and for how long, and when they would be destroyed. *Read more*

DRONES

FAA Seeking to Quicken UAS Airspace Authorization Process

The Federal Aviation Administration (FAA) recently published notice in the Federal Register seeking permission to quicken authorizations for Part 107 unmanned aircraft system (UAS) operations in restricted areas. The FAA wishes to use the Low Altitude Authorization and Notification Capability (LAANC) system for authorizations, which would give the FAA the ability "to grant near-real time authorizations for the vast majority of operations," including "Class B, Class C, or Class D airspace or within the lateral boundaries of the surface area of Class E airspace designated for an airport unless that person has prior authorization from Air Traffic Control (ATC)."

The LAANC system will soon be used at 50 U.S. airports, which will give drone operators the ability "to apply for instant, digital approval to fly in U.S. controlled airspace using the same applications they use for flight planning and in-flight situational awareness," according to AirMap. *Read more*

How Do We Control the Crowded Skies?

While the National Aeronautics and Space Administration (NASA) completed some testing and research of unmanned aircraft systems' (UAS) traffic management system, as directed by the Federal Aviation Administration (FAA), we still have a lot to learn before UAS can be safely and broadly integrated into our national airspace. To date, NASA maintains that the U.S. does not have a system in place that's going to keep UAS safely separated from each other. And if we're going beyond the line of sight of the operator, we don't have all the bits and pieces right now in the airspace system. Regardless, NASA is set to present its UAS traffic management (UTM) program to the FAA in 2020. *Read more*

DOT Announces Drone Pilot Program to Encourage Local and National Collaboration

President Donald Trump has directed the U.S. Department of Transportation (DOT), in partnership with state and local governments in select jurisdictions, to launch an initiative that will safely test and validate advanced operations for drones. According to the DOT, the results of the Unmanned Aircraft Systems (UAS) Integration Pilot Program will be used to speed up the safe assimilation of drones into national airspace, which will in turn showcase the benefits of this emerging technology in the U.S. economy. *Read more*

PRIVACY TIP #112

LG Releases IoT Software Update

Security researchers at Check Point discovered software vulnerabilities in LG IoT devices, which allowed them to potentially gain control over LG refrigerators, ovens, dishwashers, and a live feed from a robot vacuum cleaner. A vulnerability in the mobile app and cloud app allowed them to remotely gain access to LG IoT devices with just an email address for authentication.

A person who is able to remotely access these appliances can turn them on or off and access individuals' information stores on the IoT devices. According to the researchers, if hackers are able to hack into individual IoT devices, they can also hack into networks of these devices, which potentially means millions of home appliances. Turning on ovens or shutting off refrigerators, or having access to home designs through vacuum cleaners could wreak havoc on millions of households with one hack.

LG issued an update to its IoT software on September 29, 2017. If you received notice of the update, or own an LG IoT device or appliance, consider updating the software on your appliance.