Robinson+Cole

# Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

**January 5, 2017**

## CYBERSECURITY

### Three Chinese Citizens Charged with Hacking New York Law Firms

Preet Bharara, the U.S. Attorney for the Southern District of New York, announced that three Chinese citizens have been charged for attempting to hack into seven law firms involved in mergers and acquisitions to pilfer information to use for insider trading. *Read More*.

---

### KillDisk a Threat for Industrial Control Systems

A new variant of the KillDisk malware is reportedly able to encrypt files and hold them for ransom instead of deleting them. Although KillDisk has been used in attacks aimed at industrial control systems (ICS), experts are now concerned that threat actors may be introducing ransomware into the industrial domain. *Read More*.

---

## DATA BREACH

### Trading Card Maker Topps Notifies Customers of Data Breach

According to several media outlets, Topps, whose products include sports trading cards, recently notified customers via email of a security breach. Information that may have been compromised includes bank account numbers, names, and email addresses of customers who placed orders between July 30 and October 12, 2016. Topps has not publicly released the number of individuals whose information may have been compromised but is offering a year of identity theft protection for customers who may have been affected. *Read More*.

---

**FEATURED AUTHORS:**

Linn Foster Freedman
Pamela H. Del Negro
Kathleen M. Porter
Kathryn M. Rattigan

**FEATURED TOPICS:**

Cybersecurity
Data Breach
Enforcement + Litigation
Drones
Privacy Tip

---

**VISIT + SHARE:**

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

**Medical Marijuana Dispensary Applications Exposed in Cyber Attack**

The Nevada Division of Public Health has announced that its Medical Marijuana Program's online database has suffered a cyber-attack that has exposed 11,700 applications requesting approval to open a medical marijuana dispensary. *Read More*.

---

**Massachusetts Data Breach Notification History Now Available Online**

The Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) has published an online list of data breach notifications issued each year to Massachusetts residents since 2007, the inception of the Commonwealth's data breach notification law. The list identifies the entity that was breached; the number of Massachusetts residents affected; whether the breach was of electronic or paper records; whether social security, drivers' license, credit, or debit card numbers were accessed; whether the data was encrypted; whether a mobile device was lost or stolen; and whether credit monitoring or other relief was offered to the individuals affected. *Read More*.

---

**ENFORCEMENT + LITIGATION**

**Amazon's Echo May Possess Evidence in a Murder Case**

Police in Bentonville, Arkansas, are seeking records from an Amazon Echo device (for the second time) which may contain records in connection with a murder investigation in the home of James Andrew Bates where Victor Collins was found dead in Bates' hot tub last year. Echo is an always-on digital assistant that can answer questions, order items, stream music, control your smart home and perform many other tasks. It is supported by an Amazon voice recognition program called Alexa, which operates via the cloud. "Always-on" does not mean always-recording. It is always listening for its "wake word", which by default, is the name of the voice recognition program, Alexa. The Echo only keeps 60 seconds of a recorded sound in a room –as a new sound is recorded, the old sound is erased. Only once the Echo hears its wake word (Alexa) does it begin streaming audio and recording the requests. Users can log into their account and erase their voice recordings and it is also possible to turn the microphone off. *Read More*.

---

**DRONES**

**FAA Approves Beyond-Visual-Line-of-Sight Operations at North Dakota UAS Test Site**

Last week, the Federal Aviation Administration (FAA) approved beyond-visual-line-of-sight (BVLOS) unmanned aircraft systems (UAS or drone) operations at a test site in North Dakota. With this approval, operators can now develop, test, and evaluate new applications for UAS technology at the Northern Plains UAS Test Site. North Dakota Senator John Hoeven said, “This authorization will help companies like General Atomics, Northrop Grumman and future tenants at the Grand Sky technology park test and evaluate complex UAS operations possible nowhere else in the nation.” Senator Hoeven also said that BVLOS operations may also encourage government agencies like NASA, the U.S. Air Force, and the Department of Homeland Security to bring UAS integration efforts to North Dakota. The Northern Plains UAS Test Site will use a chase plane until the Grand Sky technology park completes a software update that will link the test site to the Grand Forks Air Force Base’s digital radar system. The digital radar system will help operators monitor UAS that fly BVLOS.

---

**PRIVACY TIP #68**

**Protecting Biometric Information**

Breaches of our personal information through hacking of databases are becoming all too common. A third of Americans’ personal information was compromised in health care breaches in 2015. We have become numb to the fact that our personal information from forms and other information shared between companies is now on the dark web, and we are all the more vigilant in protecting our identity, knowing it is easily accessible.

The use of biometrics is becoming the standard for authentication. It is touted to increase the security in accessing one’s smartphone and banking applications through a fingerprint, and iris scans are used in employment and defense operations and for contractors. These uses of biometrics are for security and for good reasons.

When you give your biometric information, and it is maintained or stored online, it is at risk, just like your personal information. Treat your biometric information carefully and protect it from use, disclosure, and exposure to compromise.

It is becoming common for professional sports arenas to allow patrons to use biometric information in security lines to get into games through a fast track—much like the TSA precheck at an airport. The difference is that, when you provide the TSA with your fingerprints, it

is presumably being used for security purposes only.

When you give your fingerprints or iris scan to staff at a professional stadium so you can get to your seat more quickly, there is no understanding of or prohibition on how they can use it or sell it or, more importantly, how they will protect it. They can sell it to other companies and track your attendance and purchases, and if it is in a database, it can get hacked. It's one thing to have your name, address, date of birth, and even your Social Security information compromised, but it is quite a different story when it is a fingerprint or iris scan. You only have one of each, and a security freeze can't protect you or bring it back.

I admit that I love sports (especially hockey) and love to attend games. But there is no way I will ever give my fingerprints or iris scan to anyone so I can get to my seat a few minutes earlier. Just get to the game earlier. Stand in line and people watch—there's no better place than at a sports arena. Fight the urge to give your biometric information and fast track it to your seat. Vigilantly protect your biometric information from use, disclosure, and compromise.