

**Robinson+Cole**

## Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks



### CYBERSECURITY

#### [Class Action Suit Filed Against Allscripts for Ransomware Attack](#)

Allscripts Healthcare Solutions Inc. notified its electronic medical record customers last week that a ransomware attack was behind the disruption of service for medical providers.

Allscripts became the victim of the ransomware “SamSam” on January 18 which shut down providers’ access to their electronic medical records. [Read more](#)

### DATA BREACH

#### [Oklahoma State Hack Compromises Half a Million Records](#)

Oklahoma State University Center for Health Sciences (OSUCHS) has notified 279,865 patients that their protected health information may have been compromised as a result of a hacking incident.

OSUCHS has determined that an unauthorized individual gained access to its system housing Medicaid billing information on November 7, 2017, but it is unable to determine whether the information was actually accessed by the intruder. [Read more](#)

### DRONES

#### [EPIC’s Standing Questioned in FAA Case](#)

On January 25, 2018, oral arguments were heard in *Electronic Privacy Information Center (EPIC) v. the Federal Aviation Administration (FAA)* case by a D.C. Circuit panel. The court questioned EPIC’s standing to contest the FAA’s regulations, which cover all Americans. EPIC alleges that the FAA’s omission of privacy safeguards in its small unmanned aerial systems (UAS) rule violates its congressional mandate to regulate UAS “hazards.” [Read more](#)

February 1, 2018

#### FEATURED AUTHORS:

[Linn Foster Freedman](#)  
[Kathryn M. Rattigan](#)

#### FEATURED TOPICS:

[Cybersecurity](#)  
[Data Breach](#)  
[Drones](#)  
[Privacy Tip](#)

#### VISIT + SHARE:

[Insider Blog](#)  
[R+C website](#)  
[Twitter](#)  
[Facebook](#)  
[LinkedIn](#)

## **The Drone Market Environment – Disruption in 2018**

It seems impossible to stay on top of all the major changes that are going on in the drone industry, so here's a list of some trends to keep a close eye on this year: [Read more](#)

---

### **PRIVACY TIP #124**

#### **FTC Alerts Consumers to Social Security Administration Scammers**

The Federal Trade Commission (FTC) issued a scam alert this week notifying consumers that it has received an uptick in complaints that scammers are calling consumers claiming they are from the Social Security Administration.

The scammers tell the individual that there has been a computer problem at the Social Security Administration and they need to confirm the individual's Social Security number.

The FTC warns consumers to never give their Social Security number over the phone to anyone they don't know. The Social Security Administration asks consumers to contact its Fraud Hotline at 1-800-269-0271 in the event that a person is contacted by someone claiming to be from the Social Security Administration.

The FTC states to never trust a name or phone number, as these scammers are able to make it look like they are calling from Washington, D.C., when in fact they are using technology to make it look that way but may be calling from anywhere in the world.

Scammers have also set up fake websites to look like legitimate websites for people to apply for a new Social Security card. These websites ask individuals to input their personal information, and then the scammers steal the information. According to the FTC, check the website to make sure that it is ssa.gov and does not re-direct you to another site.

Scammers continue to try creative ways to dupe consumers into providing their personal information to them. They continue to be successful, taking advantage of honest and innocent people. These warnings are helpful to remind us all to protect our personal information from theft.