Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

New York Cybersecurity Regulation Delayed

The New York Department of Financial Services (NYDFS) will delay the effective date of its proposed cybersecurity regulation until March 1, 2017. A new draft will be published on December 28, 2016, with an anticipated 30-day comment period. The original proposed regulation was met with significant resistance, including reportedly more than 150 comment letters. Many of the comments identified the proposed regulation as highly prescriptive and lacking an allowance for covered entities to make risk-based decisions on certain important technology matters. Additionally, a number of comments requested the ability to distinguish between small and large covered entities in structuring cybersecurity programs based on size and risk. A number of the comments also expressed concern that inconsistencies with federal and other state regulations, which are anticipated in the future, would make compliance highly complicated. Nevertheless, a number of comments expressed agreement with the department's goal of improving cybersecurity programs overall. If the original 180 days for covered entities to come into compliance with the regulation is maintained, August 28, 2017, will be a crucial date. It is not known whether the department will extend the January 15, 2018, date for certification of compliance with the regulation.

Large Majority of Businesses Pay to Unlock Ransomware

2016 has been a banner year for ransomware cybercriminals. We have seen a dramatic rise in the use of ransomware, and businesses continue to become victims of ransomware, primarily through phishing and spear phishing schemes. The cybercriminals are getting so brazen that, when they attack a business with ransomware, they actually provide instructions on how to pay the ransom with bitcoin and a link.

The problem is that businesses who are victimized continue to pay the criminals, as often it is cheaper to pay than to try to get their systems back up and running. *Read more*

December 22, 2016

FEATURED AUTHORS:

Kelly Frye Barnett
Richard M. Borden
Linn Foster Freedman
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Children's Privacy
Data Breach
Data Privacy
Drones
Enforcement + Litigation
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

ENFORCEMENT + LITIGATION

DeVry University Settles with FTC for a Whopping $100 Million

The Federal Trade Commission announced this week that it has settled with DeVry University [view related post] for $100 million over allegations that it misled prospective students with ads that promised higher employment success and income upon graduation. The settlement required DeVry to pay $49.4 million in cash to qualified students who were harmed by the deceptive ads and $50.6 million in debt relief for students. *Read more*

Shareholders Derivative Suit Filed against Wendy's for Data Breach

Continuing the trend of filing a shareholders derivative suit following a data breach, a Wendy's shareholder recently filed a derivative suit against Wendy's executives and board members alleging they did not adequately protect data from a breach. *Read more*

Tum Settles Allegations by the FTC for Deceptive Advertising Tactics

Tum, Inc. (Tum), a California-based company that enables sellers to target digital advertisements to consumers via a website or mobile app, settled allegations by the Federal Trade Commission (FTC) that it deceived consumers by tracking them online and through their mobile app even after consumers opted out of such tracking. *Read more*

DATA PRIVACY

Report Urges Policymakers to Increase Protections for Consumer Data Collected through Wearable Devices

A 122-page report was published this week by American University and the Center for Digital Democracy that examines features, key players, and trends that are emerging in consumer-wearable and connected-health devices. *Read more*

DATA BREACH

November the Worst Month Yet for Health Care Breaches

We previously issued numerous warnings to the health care industry about malware and ransomware [see related posts here and here]. Our predictions have unfortunately come true, as, according to self-reports to the Office for Civil Rights (OCR) November was the worst month ever for health care data breaches. In the month of November, 57 incidents of unauthorized access, use, or disclosure of protected health information were self-reported to the OCR. *Read more*

CHILDREN'S PRIVACY

Toys Not Immune from Scrutiny over Privacy and Security Weaknesses

In the wake of the holiday season, it seems that even toys are not immune from privacy and security pitfalls. Two "connected" toys, Genesis Toys' My Friend Cayla and i-Que robot, have been accused of violating U.S. and European privacy, security, and advertising laws. *Read more*

DRONES

How Can You Mitigate Risks When Flying a Drone Beyond Visual Line of Sight?

Precisionhawk, one of the leaders in the drone market, released a report this week outlining operational risks when flying drones beyond the visual line of sight (BVLOS). Precisionhawk's director of airspace research, Dr. Allison Ferguson, said, "While we believe that technology would be useful for flying BVOLS, we needed a quantitative answer as to whether it would simply make the user's life easier or it actually impacted the safety of the operation. The FAA needs a clear understanding of the risks associated with advanced drone operations, and [our] testing sets a visual baseline to measure the level of safety as we add enabling technologies." *Read more*

Amazon's First Drone Delivery

Amazon's Prime Air took off on its first fully autonomous package delivery flight. Amazon's website included a video and post about its first flight, writing, "We're excited about Prime Air–a delivery system designed to safely get packages to customers in 30 minutes or less using unmanned aerial vehicles, also called drones. Prime Air has great potential to enhance the services we already provide to millions of customers by providing rapid parcel delivery that will also increase the overall safety and efficiency of the transportation system." *Read more*

Tips for Implementing Drones in Public Safety

The Office of Justice Programs' (OJP) National Institute of Justice (NIJ) released a report this week examining issues related to the use of unmanned aerial systems (UAS or drones) for public safety purposes. "Considerations and Recommendations for Implementing an Unmanned Aircraft Systems (UAS) Program" concludes that, while drones are beneficial in assisting law enforcement in many ways, the technology also brings the concern of police violating privacy rights through aerial surveillance. *Read more*

PRIVACY TIP #66

False IRS Phone Scams Defraud Victims of More than $50 Million

We have previously warned consumers about IRS phone scams that defraud consumers.

Basically, the fraudsters, impersonating an IRS official, call unsuspecting victims over the telephone, and intimidate the recipient of the call to believe they have an outstanding tax liability, telling them that if they don't pay up, they will be arrested and go to jail. It's quite a scary thought. And aren't we all inherently afraid of the IRS? These fraudsters know this and take advantage of it.

Despite multiple warnings by the IRS, these schemes continue to victimize consumers and are estimated to have cost victims more than $50 million.

This week, the Federal Communications Commission (FCC) issued a public notice alerting consumers that it is working with the Treasury Inspector General for Tax Administration, and together they are "committed to quashing the scam, prosecuting the individuals behind the scam and protecting consumers from future fraud and harassment."

The notice reminds the public that impersonating an IRS agent and telephone fraud are both crimes that are punishable by fines and imprisonment.

The FCC reminds consumers that the IRS does not request payment of taxes over the telephone and does not request payment on iPhone cards, gift cards, or wire transfers.

This writer agrees with the FCC that consumers should not engage with these callers and should hang up on anyone claiming to be an IRS official. The IRS will not call you.

Beware of this scheme and others like it, and don't fall for it. Don't increase the profit for these fraudsters who prey primarily on the elderly. And on that note, spread the word to your family and friends

too. We need to have each other's backs to combat this scheme.