Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Russians Continue to Attack U.S. Energy and Power Sectors

Late last week, a joint statement by the Department of Homeland Security and the Federal Bureau of Investigation confirmed that the Russian government has been behind an ongoing targeted campaign to penetrate U.S. power plants and the electric grid. *Read more*

The Report to the President for "Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats"

Back in January, a draft report from the U.S. Department of Commerce and the U.S. Department of Homeland Security was released to President Trump to address his May 11, 2017, Executive Order, which called for strengthening "Cybersecurity of Federal Networks and Critical Infrastructure." *Read more*

DATA PRIVACY

Facebook and the English Data Firm Cambridge Analytica (CA) Face Intense Scrutiny for Possible Misuse of Facebook User Data

Facebook and the English data analytics firm Cambridge Analytica (CA) are facing intense scrutiny in response to numerous reports about the possible misuse of data of 50 million Facebook accounts. The data was originally collected through a third party personality test app and later reportedly improperly transferred to CA and/or its parent company Strategic Communications Laboratories (SGL) and used to create target voters as part of CA's political campaign consulting business. *Read more*

March 22, 2018

FEATURED AUTHORS:

Kelly Frye Barnett
William M. Daley
Linn Foster Freedman
Kathleen M. Porter
Joanne J. Rapuano
Kathryn M. Rattigan

FEATURED TOPICS:

Automated Vehicles
Cybersecurity
Data Breach
Data Privacy
Drones
Enforcement + Litigation
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

U.S. Citizen Sues Cambridge Analytica in U.K. Courts for Violations Under U.K. Data Protection Act

On March 16, David Carroll, a New York based American professor, sued Cambridge Analytica (CA) in the U.K. courts, after the data analytics firm allegedly failed to respond to his request made pursuant to the U.K. Data Protection Act for his file of personal data held by CA, CA's purpose for processing his data, and the persons and countries outside the E.U. with whom his data was shared. *Read more*

DATA BREACH

Orbitz Confirms Breach of Travel Records and Credit Card Information of 880,000 Individuals

Orbitz, the travel booking entity owned by Expedia, has confirmed that it has "identified and remediated a data security incident affecting a legacy travel booking platform." This means one of its older websites used by customers to book their travel plans was hacked. The statement says that Orbitz uncovered evidence earlier this month that an attacker had access to the legacy system between October and December 2017, and the information of travel booking customers was compromised if they made any purchases through the legacy website between January 2016 and December 2017. *Read more*

ENFORCEMENT + LITIGATION

Recent Supreme Judicial Court Decisions Highlight How Courts Must Embrace Technological Change

Courts are often faced with the dilemma of applying centuries, or even decades, old law to constantly evolving technological advancements. See, e.g., Transcript of Oral Argument, *United States v. Microsoft*, No. 17-2 (U.S. Feb. 27, 2018) (attempting to ascertain the relationship between the Stored Communications Act, a 1986 law, and modern cloud computing and storage capabilities—which simply did not exist in 1986) (available here). In a series of decisions, starting with *Commonwealth v. Dorelas*, the Massachusetts Supreme Judicial Court has addressed the constraints of law enforcement's ability to conduct searches of digital storage devices—like cell phones. 473 Mass. 496, 43 N.E.3d 306 (2016). In *Dorelas*, a divided 4–3 Court held that photographs from a defendant's iPhone were admissible when obtained pursuant to a broadly worded warrant that allowed officers to search the device for threatening communications. *Read more*

DRONES

Northwell Health Seeks to Use Drones and Telehealth for Emergency Care

Northwell Health, a New York-based health system, is seeking to use a fleet of emergency drones, in combination with telehealth technology, to respond to accidents more quickly, treat opioid overdoses, and even provide medical attention needed due to terrorists attacks. However, there are still a lot of barriers to burst through before Northwell Health can carry out these plans.

Purna Prasad, Ph.D., Chief Technology Officer at Northwell Health, said, “This is actually our next foray into telehealth. There may be places where there is no network connection, or there may be places where people just don’t have the wherewithal to have any of type of mobile phone for two-way video conferencing. *Read more*

FAA Releases FY 2018-2038 Aerospace Forecast; Drones in Our Future

The Federal Aviation Administration (FAA) released its Fiscal Years 2018-2038 Aerospace Forecast last week, indicating, among other things, that the FAA expects small model hobbyist unmanned aerial systems (UAS or drones) to more than double from 1.1 million in 2017 to 2.4 million by 2022, while the commercial drone fleet will grow from 110,604 in 2017 to 451,800 by 2022. This is a growth rate of over 16 percent over that five-year period for hobbyist drones and a growth rate of over 32 percent for commercial drones. *Read more*

First U.S. Test Flights Completed by Drone Delivery Canada

Drone Delivery Canada (DDC) of Toronto completed a series of successful drone delivery test flights at the beginning of this month in Rome, New York at the Griffiss International Airport. These drone delivery test flights were the first conducted by DDC in the United States. DDC used its Transport Canada-compliant Sparrow Drone (with a lift capacity of about 11 lbs.), its proprietary FLYTE management system and its proprietary DroneSpot technology to conduct the flights. Chief Technology Officer of DDC, Paul Di Benedetto, said, “Testing at Griffiss was a natural extension for continued progress with our platform in [beyond visual line of sight], non-segregated airspace environment. An active runway with large aircraft, helicopters, and general aviation aircraft is the latest advancement to our operations team airspace integration efforts and a progression from the knowledge learned during DDC’s [prior]

operations." These test flights had a 100 percent success rate. *Read more*

Trump Policy on Unmanned Military Aircraft Expected to Allow Export of Lethal Drones

President Donald Trump is expected to ease up on the rules related to foreign sales under a new policy on unmanned military aircraft as part of a broader overhaul of arms export regulations under the "Buy American" initiative. The new policy could make it easier to export some types of lethal U.S.-manufactured drones to U.S. allies. This is good news to many U.S. drone manufacturers who are facing surging competition overseas from Chinese and Israeli manufacturers who often sell their drones under lighter restrictions. On the other side, human rights and arm control advocates worry that this policy change will only fuel violence and instability in regions such as the Middle East and South Asia. *Read more*

AUTOMATED VEHICLES

Self-Driving Uber Vehicle Kills Pedestrian in Arizona

This week, a self-driving SUV operated by Uber—and with an emergency backup driver behind the wheel—struck and killed a 49-year-old pedestrian as she walked her bicycle across a street in Tempe, Arizona. It is believed to be the first pedestrian death associated with self-driving technology. In addition to the Tempe Police Department, the National Transportation Safety Board said it was sending a team of four investigators to determine "the vehicle's interaction with the environment, other vehicles and vulnerable road users such as pedestrians and bicyclists." Data from the vehicle's many cameras and sensors will no doubt prove useful to the investigations. *Read more*

PRIVACY TIP #131

Bryant University Women's Summit Follow-Up

I was so honored to be a presenter at the Bryant Women's Summit last week. It is always an incredible event, and I enjoy attending every year. But the bonus for me this year is that I also got to interact with a lively group of executive and professional women who were eager to learn about the topic: "Take Control of Your Personal Information: Understanding the Risks and Rewards of Using Smartphones, Mobile Applications, and Social Media."

These powerhouse women kept me on my toes the entire time! They were eager to learn about the mine fields presented by the camera,

microphone, and location based services settings on their smartphones, about online banking risks, privacy settings with social media accounts, how digital personal assistants are collecting biometric data of children, the mining of data by internet service providers and email platform providers, and the aggregation of personal information by companies and how they are using and monetizing personal information.

There were a couple of questions presented that I promised to address during the Privacy Tip this week, including providing sites to access related to specific questions asked during the session.

1. “How do I find out if my information has been compromised?”

I wrote about www.haveibeenpwned.com during a previous Privacy Tip [view here]. Check out the post and the site to see if your email address and/or other information have been compromised.

2. “How do I know if someone has stolen my identity?”

One of the first things to do to see if anyone has used your personal information to open up an account under your name is to obtain a copy of your credit report. Every individual in the U.S. is entitled by law to obtain a copy of his or her credit report for free from each of the credit reporting agencies (Experian, TransUnion and Equifax) annually. That means you can get three free credit reports a year—one from each company.

In order to obtain your credit report, you can go to either the Federal Trade Commission website (www.ftc.gov) or Consumer.ftc.gov which outline information for consumers on how to get their free credit report. Additionally you can go directly to www.annualcreditreport.com or call 1-877-322-8228. Yes, you have to give your personal information, including your Social Security number so they can authenticate you. And yes, they already have it.

Note that there are scam websites out there that spoof annualcreditreport.com, so don’t be fooled and go through the FTC website to be sure it’s the correct site. Here is a previous blog post about the importance of obtaining your credit report annually to keep a tab on all accounts that are in your name.

3. “How do I find out about scams before I become a victim?”

A great resource is the Federal Trade Commission. One of its missions is to protect consumers. The FTC issues scam alerts that you can subscribe to, which will inform you of the latest potential scam of threat. You can subscribe to the scam alerts by going to the FTC website www.ftc.gov. I also frequently check the FBI and IRS websites. And of course, subscribe to Robinson+Cole’s Privacy + Cybersecurity blog. We work to alert consumers on all the latest attacks and potential threats in real time.

Thanks again to Bryant University for hosting this wonderful event year after year, and for those who attended my session—it was so enjoyable!