Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

DOD U.S.-CERT Cybersecurity Incident Reporting for Defense Contractors Effective April 1, 2017

New U.S. Computer Emergency Readiness Team (U.S.-Cert) guidelines around incident reporting went into effect this week (April 1, 2017). The guidelines require all federal departments and agencies; state, local, tribal, and territorial government entities; information-sharing and analysis organizations; and private sector organizations to report any security incident impacting the confidentiality, integrity, or availability of a federal government information system to U.S.-Cert within one hour of the incident. *Read more*

IBM Issues 2017 X-Force Threat Intelligence Index Findings

Last week, IBM published its X-Force Threat Intelligence Index (Index), which summarizes the state of leaked records and vulnerabilities to data in 2016. It is depressing but informative. The Index notes that the number of compromised records "grew a historic 566 percent in 2016 from 600 million to more than 4 billion." But more significantly, the Index found that cybercriminals are getting more creative in their strategies and are now focusing on unstructured data, including email archives, business documents, source code, and intellectual property. *Read more*

DATA SECURITY

FAFSA Data Retrieval Tool Remains Down Over Security Concerns

Last week, the Internal Revenue Service (IRS) and Federal Student Aid (FSA) announced that the Data Retrieval Tool (DRT) on fafsa.gov and StudentLoans.gov will be unavailable until extra security protections could be added. Since 2010, students have been able to use the DRT to transfer tax data directly into the Free Application for Federal Student Aid (FAFSA). In early March, the DRT was disabled after it was discovered that identity thieves may have used personal information obtained outside the tax system to access the FAFSA form in an attempt to obtain tax information. The IRS is continuing to

April 6, 2017

FEATURED AUTHORS:

Kathleen E. Dion
Linn Foster Freedman
Kathleen M. Porter
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Enforcement + Litigation
Data Breach
Data Privacy
Data Security
Drones
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

investigate whether this use of the tool contributed to fraudulently filed tax returns. *Read more*

DATA PRIVACY

FCC Broadband Privacy Regulations Rescinded; States Consider Adopting Measures

As was expected [see previous post], President Trump signed into law the rescinding of the broadband privacy regulations adopted in 2016 by the Obama administration's Federal Communications Commission (FCC). The now-rescinded regulations would have required Internet service providers (ISPs) to obtain consent from a customer before using or selling the customer's Web browsing history, app usage history, precise geolocation, financial information, health information and children's information for advertising purposes. *Read more*

DATA BREACH

Job Seekers Beware! Data Hacked for up to 1.4 Million Illinois Residents Receiving Unemployment Benefits

The Illinois Department of Employment Security has revealed that somewhere between 1.2 and 1.4 million Illinois residents who have received unemployment benefits from the State of Illinois have had their names, dates of birth, and Social Security numbers compromised through a hacking of its vendor's database. Illinois is in the process of notifying affected individuals. *Read more*

Job Site of McDonald's Canada Hacked

McDonald's Canada has shut down its careers webpage following a breach that occurred in mid-March. A hacker gained access to the jobs section of its website and compromised the personal information, including names, addresses, telephone numbers, employment histories, and other job application information of approximately 95,000 individuals. *Read more*

DRONES

Sense-and-Avoid Software Tests Successfully in Recent Drone Flights

The Federal Aviation Administration (FAA), Northrop Grumman, and Aviation & Communication & Surveillance Systems (ACSS) recently

announced a series of successful drone flights testing sense-and-avoid systems. One of the key issues with flying a drone beyond the visual line of sight is that the sense-and-avoid technology is slow to come to market. It is certainly out there and being used by big companies in the commercial UAS business. But, before the FAA can issue a waiver under its Part 107 regulations, it needs to know that this technology, when built into the drone, really works. After all, the FAA's first priority is safety in the national airspace. *Read more*

Commercial Drone Alliance Speaks Out against Drone Privacy Legislation

The Commercial Drone Alliance (CDA) voiced its opinion on the drone privacy legislation recently reintroduced by U.S. Senator Edward J. Markey and U.S. Representative Peter Welch. The Drone Aircraft Privacy and Transparency Act seeks to ensure transparency and privacy of unmanned aircraft systems (UAS) operations. However, the CDA argues that this bill would create an additional layer of regulation that departs from existing technology-neutral standards. CDA recommends that existing laws should apply—that is, the laws that currently apply to similar advances in photography-related technologies like photos captured by handheld cameras, smartphones, telephoto lenses, helicopters, and, now, even UAS. Current laws protect against trespassing, stalking, and peeping toms and can be applied to the UAS technology which does the same thing as these other technologies—capture video and images. *Read more*

ENFORCEMENT + LITIGATION

Rite Aid Beats TCPA Lawsuit over Flu Shot Reminder Prerecorded Calls

A group of Rite Aid customers sued Rite Aid in December 2014 for alleged violations of the Telephone Consumer Protection Act when it sent flu shot reminders to consumers' cellphones without written consent. On March 30, 2017, a federal district court judge in New York dismissed the proposed class action lawsuit by granting Rite Aid's motion For summary judgment and denied the plaintiff's motion for class certification as moot. The full opinion has not been released and will be delayed until the parties agree on appropriate redactions of confidential information. *Read more*

PRIVACY TIP #81

LastPass Users—Listen Up!

People always ask me if I use a password manager. The answer is no. I am too paranoid to put all of my passwords in one place. Instead, I prefer to use variations on complex pass phrases that I can remember and I change them frequently. I have a good memory, so it works for me.

Even though I do not use a password manager (and by password manager I do not mean a file called “passwords”), many people do. If you use LastPass as your password manager, and you read this blog, you will know that LastPass has had its share of issues.

In the past few weeks, those issues escalated when a member of Google’s Zero Day Project found some vulnerabilities in Last Pass that users should be aware of. According to reports, the issue could take some time to fix and is being described as a “major architectural problem.”

The vulnerability affects version 4.x users and would allow a phishing attacker to steal passwords from the LastPass vault when the user is directed to a malicious website. It also could execute code on the user’s computer if it is running LastPass’s binary component (autologoff, fingerprint authentication, copy username button, copy password button, allowing importing and exporting data, adding a layer of additional encryption, importingfrom Chrome, Safari, and Opera browser password managers). Ouch.

LastPass is advising its customers to launch sites from inside the vault, instead of from the toolbar or using auto-fill, and then turn on two-factor authentication sites that offer it until there is a fix.

LastPass has promised to release its analysis when it has fixed the issue and, if you are a LastPass user, you may wish to read it closely.

It should be noted that security experts are praising LastPass for its responsiveness to the recent issues, and all indications are that it its working hard to resolve the most recent one.

Nonetheless, the Privacy Tip for this week is that I would reconsider putting all of your passwords in one place.