Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

The Weekly Newsletter of The George Washington University Cyber Security Policy and Research Institute

Quick Links

About CSPRI

Contact Us

Newsletter Archive

Blog: The CSPRI Byte

Follow Us

Follow us on Twitter: @gwCSPRI

Follow CSPRI Director, Lance Hoffman: @lancehoffman1

Follow CSPRI Associate Director, Costis Toregas: @DrCostisToregas

May 26, 2015

Seven (7) Cyber security events are scheduled in the Greater Washington Area in the next few weeks.

Tech firms and experts warn on encryption policy

Last week 140 tech companies, dozens of civil liberties, human rights, and press freedom groups, and 60 security and policy experts including CSPRI's Prof. Lance Hoffman "sent a letter to President Obama warning of the unintended consequences of any policy meant to weaken the encryption technologies that protect Internet communications."Read details **here**. Read the letter **here**. **See related story (NSA Update) below.** Read a different point of view by GW Professor and CSPRI researcher AmitaiEtzioni in his May 11 article "**Ultimate Encryption**".

Legislative Lowdown

-The House Homeland Security Committee approved theHomeland Security Drone Assessment and Analysis Act, which would require the DHS to conduct a study of the threats to homeland security posed by "commercially available small and medium sized unmanned aircraft.

Cyber Security Policy News

Events

May 27-28
Smart Cities Workshop

May 28
Online Privacy & Data Security

May 28
Dealing With Cybersecurity Threats & Breaches

May 28
CharmSec Meetup

June 1-2
Takedown Con

June 1-4
Computer-aided Cryptography

June 3
DC Metro Cyber Security Summit

Click here for detailed descriptions

NSA Update

-The National Security Agency is winding down its mass-spying program, following political maneuvers on Capitol Hill aimed at curtailing the NSA's domestic surveillance activities. The National Journal reports that while Senators will return to Washington after the holiday break to have a go at one last effort to reach an agreement on the NSA's bulk surveillance activities, the White House is already shutting the program down. "Key provisions of the Patriot Act are set to expire onJune 1, but White House officials have been warning that, without congressional action, the NSA would need to begin winding down its bulk collection of millions of phone records on May 22," writes Brendan Sasso. "That was the deadline set by the Foreign Intelligence Surveillance Court, which oversees the nation's intelligence programs. The secretive court, which reauthorizes the phone data-collection every 90 days, told the administration it would need to file its new application by May 22."

Report on the FBI's use of Section 215

Separately, The DOJ's Office of the Inspector General released a report this month detailing the FBI's use of Section 215 and warning that "significant oversight" is required, reports the Electronic Privacy Information Center (EPIC). "The Inspector General describes the FBI's expanding use of 215 to collect electronic information in bulk and criticized the agency for taking seven years to develop minimization procedures," EPIC observed. "The Second Circuit ruled the NSA's telephone record collection program exceeded the legal authority under Section 215. Unless Congress votes to reauthorize or modify the authority, Section 215 is set to expire on June 1."

-The rate of major data breaches in the United States is rapidly increasing, as hackers around the world become more sophisticated, a top FBI cyber official said Thursday.

"James Trainor, acting assistant director of the FBI's Cyber Division, said the agency used to learn about a new, large-scale data breach every two or three weeks," writes The Hill. 'Now, it is close to every two to three days,' Trainor said at an event hosted by Microsoft. 'Those types of events, whether they concern a national security threat actor or a criminal actor, are ones we see on a much more regular basis.', Trainor also said the cybersecurity industry needs to "double or triple" its workforce in order to keep up with hacking threats.

Hedge funds

- The government is working with "several" hedge funds that have been victims of cyber extortionists, according to USA Today. John Carlin, head of the Justice Department's National Security Division, made the comments Friday at the SALT hedge fund conference in Las Vegas. "We are seeing nation-state action - from Russian, China, Iran and North

Korea -- target your companies and what you have, day in and day out, to use your information against you," Carlin warned the Wall Street crowd. Read more here.

DOJ's new policy on domestic use of drones
-The Justice Department last week issued a new policy on the domestic use of drones, acknowledging that the FBI, DEA and other federal law enforcement agencies are likely to make increasing use of unmanned aerial drones in the United States. The Associated Press reports that the DOJ's first written guidelines for domestic drone use and emphasized the need to respect civil and constitutional rights. "The five-page policy document comes 19 months after the agency's inspector general recommended drone-specific policies that consider privacy rights," the AP notes. "That report said that unmanned drones raised greater privacy concerns than pilot-operated aircraft because they can fly closer to homes and operate for days at a time."

US Cyber Command cancels outsourcing contract
-The U.S. Cyber Command is canceling a $475 million contract to outsource support for cyberspying and network attacks against foreigners, according to NextGov. "As of Fridayafternoon, there were few details on why the five-year-old command, which is racing to staff up, revoked an April 30 request for proposals from contractors," writes Aliya Sternstein. "The jobs were worth up to $475 million over five years."

RadioShack update
-RadioShack Corp. won court approval to sell data on about 67 million customers in a $26.2 million deal for assets that also includes the bankrupt electronics retailer's name.
Almost 40 states, led by Texas, reached an agreement with the chain and the buyer limiting the use of the shopper data. According to Bloomberg Business, the states had expressed concern about how Standard General might use the information.

About this Newsletter

This newsletter is a weekly summary of events related to cyber security policy and research, with a special focus on developments and events in the Washington, DC area. It is published by the Cyber Security Policy and Research Institute (CSPRI) of the George Washington University. CSPRI is a center for GW and the Washington area that promotes technical research and policy analysis of topics in or related to cybersecurity. More information is available at our website, http://www.cspri.seas.gwu.edu

CSPRI

202 994 5613. cspri@gwu.edu
Tompkins Hall, Suite 106
725 23rd Street NW
Washington DC, DC 20052