Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

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

In This Issue

Quick Links

Opinion

The Crypto Policy Debate Redux and a Possible Way Forward
Lance J. Hoffman,
CSPRI Director

"I feel like I have been transported back 20 years in time. Comments made by FBI Director James Comey and Attorney General Eric Holder, Jr. against the use of stronger encryption by Apple and Google and responses from the computer industry

October 13, 2014

Twelve (12) Cyber security Events are scheduled in the Greater Washington Area in the few weeks.

Announcements

CSPRI, in the School of Engineering and Applied Science, has joined a cooperative effort with the School of Media and Public Affairs in the Columbian College of Arts and Sciences, the Institute for International Economic Policy in the Elliot School of International Affairs, and the Law School to present a seminar, **Emerging Issues in Internet Freedom and Governance**, that covers interrelated areas of international Internet policy that are prominent in public and scholarly debate and will shape the contours of the future global Internet. Running themes include the tensions between freedom and (cyber)security, privacy and publicity, and commercial development and the public good. The series events frame the underlying issues and address competing prescriptive measures, such as industry self-regulation and transparency reporting, as well as the technological implications and constraints. Click to see events, schedule, supporting background material, etc.

Events

Click here for descriptions of the upcoming events!

Click the Calendar to See Upcoming Events at a Glance!

CSPRI in the News

In the Washington Post

CSPRI Director Dr. Lance Hoffman was featured in the Washington Post in their "Letters to the Editor" section, discussing smartphone encryption.

Read the letter here.

Read a related story in the Opinion section on the left-hand side of this

(and others) about the importance of privacy and of customer trust echo the Great Clipper Chip Debate in 1993-1994. Many of the very same issues were being discussed and the same arguments were being made then as now. Even the same solution -- cryptographic key escrow - is being proposed, just as it was in 1993 by the National Security Agency."

Read more.

Legislative Lowdown

-The White House has significantly pared down its expectations for passing any omnibus cybersecurity legislation this year, and has instead focused on chopping up the legislation into bite-size chunks that lawmakers are more likely to approve, the White House cybersecurity czar said Thursday. As USA Today reports, White House Cybersecurity Coordinator Mitch Daniels said the administration will now focus on "getting whatever we can passed" using whatever legislative vehicle is available. He said it will be tough to make that happen this year, meaning the issue will likely be punted to the new Congress in January.

Cyber Security Policy News

The Right to be Forgotten
-A hefty number of Europeans are taking advantage of a new legal right to force Google to delete search results about them, writes Brendan Sasso for National Journal. "Since the process began several months ago, Google has received 144,954 requests to delete 497,695 pages from its search engine, the company revealed in a report Friday. "But Google actually rejected most of the requests under the 'right to be forgotten. The company granted 41.8 percent of the requests to scrub links." Perhaps unsurprisingly, Facebook was the most common site that people tried to hide from search results, while Google's own YouTube came in third. France, Germany, and the United Kingdom were the top sources of requests to delete links, the report found.

National security letters
-A federal appeals court last week struggled with the legality of the secrecy cloak the FBI has thrown over its use of national security letters to gather information from Internet providers and telecommunications companies, reports the San Jose Mercury News. "During nearly an hour of arguments, a three-judge 9th U.S. Circuit Court of Appeals panel sent no clear signal on whether it would strike down a provision in the Patriot Act that allows the FBI to send the letters in anti-terrorism and domestic spying probes and bars recipients from disclosing them," writes Howard Mintz. "The appeals court appeared troubled that the federal government has not taken steps to rid the law of its First Amendment problems, particularly in light of a 2008 New York federal appeals court ruling that gave guidance in a similar legal challenge."

Hotel admits to blocking WiFi
-A hotel in Tennessee has agreed to pay $600,000 to the Federal Communications

newsletter.

Follow Us

Follow us on Twitter:
@gwCSPRI

Follow CSPRI Associate Director, Costis Toregas:
@DrCostisToregas

Follow CSPRI Research Scientist, Allan Friedman:
@allanfriedman

Commission (FCC) after it was found that the establishment was blocking customers' mobile WiFi hotspots in a bid to make them pay to use the hotel's Internet services. As Ars Technica reports, the Gaylord Opryland hotel in Nashville admitted to the FCC that "one or more of its employees used containment features of a Wi-Fi monitoring system at the Gaylord Opryland to prevent consumers from connecting to the Internet via their own personal Wi-Fi networks," writes Cyrus Farivar. "That hotel sells dedicated wireless services and custom networks for convention purposes at prices ranging from $250 to $1,000 per access point. But on that same setup is a 'monitoring system' that allows the company to effectively shut down any other Wi-Fi networks that are not their own, such as one produced by a MiFi or similar personal portable Wi-Fi device. The FCC found that this feature was in violation of one of its own advisories that forbids blocking, jamming, or interference with authorized radio communications, including Wi-Fi."

DHS will proactively monitor for cyberthreats
- The Department of Homeland Security has signaled its intention to proactively monitor civilian federal agency networks for signs of cyberthreats. NextGov reports that move comes after agencies arguably dropped the ball this spring in detecting federal websites potentially harboring the Heartbleed superbug. "Annual rules for complying with the 2002 Federal Information Security Management Act released Friday require agencies to agree to proactive scanning," writes Aliya Sternstein. "The regulations also contain new requirements for notifying DHS when a cyber event occurs."

Executives are placing a value on the importance of cybersecurity
-Cybersecurity has emerged as a top issue for executives surveyed in Government Technology's 2014 Digital States Survey; according to the publication, 65 percent put cybersecurity in among their top three priorities. But why is this notable from previous years, when the topic also emerged as a top concern for respondents? GovTech believes it's because the issue hasn't been on the radar of top management, but rather has been perceived "as a problem for the technology guys to fix, not a risk for leadership to address. That's changing now as more and more of us become victims of data theft," writes Steve Towns. "A recent report from CNNMoney estimates that nearly half of all adults in the U.S. have had personal information stolen by hackers in the last 12 months, and it's reasonable to think that many of them are asking why top execs aren't taking better care of their data."

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
304 Staughton Hall
707 22nd St., NW
Washington DC, DC 20052