

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](#)

[Announcements](#)

[Legislative Lowdown](#)

[Cyber Security Policy
News](#)

[Events](#)

Quick Links

[About CSPRI](#)

[Contact Us](#)

[Newsletter Archive](#)

[Blog: The CSPRI Byte](#)

October 27, 2014

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

Of note this week...

Cybersurveillance: New Snowden Video Interview and New Snowden Documentary

On October 20, Harvard Law School Professor Lawrence Lessig interviewed Edward Snowden. Click [here](#) to see the entire interview.

And Godfrey Chesire, in [rogerebert.com](#), called Laura Poitras' film Citizenfour about Snowden "the movie of the century (to date)." It's been playing to packed houses at Washington's E Street Cinema.

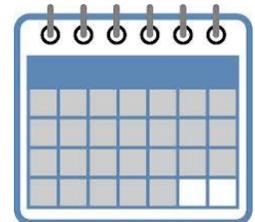


Edward Snowden and girlfriend in Moscow
(from *Citizenfour*)

Events

Click [here](#) for descriptions of the upcoming events!

Click the Calendar to See Upcoming Events at a Glance!



Follow Us

Follow us on Twitter:
[@gwCSPRI](#)

Follow CSPRI Director,
Lance Hoffman:
[@lancehoffman1](#)

Follow CSPRI Associate
Director, Costis Toregas:
[@DrCostisToregas](#)

Follow CSPRI Research
Scientist, Allan
Friedman:
[@allanfriedman](#)

Legislative Lowdown



-Despite the number of cyber-focused bills on Capitol Hill right now, Congress is unlikely to move anything forward any time soon, according to ThreatPost. "More than a year out from Snowden, and closing in fast on another presidential election, the prospects for legislation are slim to none with a lame-duck president in office and a new Congress due in January," [writes](#) Michael Mimoso. Some of the bills that seemed to have the biggest momentum this year included curbs on the NSA's domestic surveillance activities, privacy reforms and a national data breach disclosure law.

Cyber Security Policy News

Florida rules on cell phone data

-The Florida Supreme Court ruled Thursday that obtaining cell phone location data to track a person's location or movement in real time constitutes a Fourth Amendment search and therefore requires a court-ordered warrant. As Wired.com [reports](#), "police departments around the country have been collecting phone metadata from telecoms and using a sophisticated spy tool to track people through their mobile phones-often without obtaining a warrant. But a new ruling out of Florida has curbed the activity in that state, on constitutional grounds. It raises hope among civil liberties advocates that other jurisdictions around the country may follow suit."

Cyber vulnerability ranks as a top risk

- Cyber vulnerability is now seen as the top risk to the broader economy, according to a new [survey](#) of financial services representatives by the Depository Trust and Clearing Corporation. Politico writes: "A record high 84 percent of respondents to the DTCC's Systemic Risk Barometer named cyber as one of their top five risks - a 25 percentage point increase since March 2014."

-The U.S. Justice Department says it is reorganizing itself to focus more centrally on cybercrime, and the changes may bring new federal court cases around cyber breaches and crime, Reuters reports. "The revamp, led by Assistant Attorney General John Carlin, also marks a recognition that national security threats have broadened and become more technologically savvy since the 9/11 attacks against the United States," [writes](#) Aruna Viswanatha. "The agency is also renaming its counter-espionage section to reflect its expanding work on cases involving violations of export control laws, Carlin confirmed in an interview. Such laws prohibit the export without appropriate licenses of products or machinery that could be used in weapons or other defense programs, or goods or services to countries sanctioned by the U.S. government."

Federal Communications Commission

-Move over Federal Trade Commission: There's a new data security cop on the beat. According to The Hill, the Federal Communications Commission is getting in on the act. "Two small phone companies will be fined a combined \$10 million

for violating their customers' privacy," The Hill's Julian Hatter [writes](#). "The FCC alleged...that TerraCom and YourTel America stored 300,000 subscribers' names, addresses, Social Security numbers, driver's licenses or other sensitive data on unguarded Internet servers that could easily be accessed anywhere in the world."

Russia to sign cybersecurity agreement with China

-Russian President Vladimir Putin is close to approving a cybersecurity cooperation agreement with China, according to Russian media reports. The agreement would call for the two countries conduct joint cybersecurity operations, according to [Russian news agency RT](#). The treaty, expected to be signed the second week of November, would require both countries to avoid using information technology to infringe on an independent state's sovereignty, government or economy.

The Enhanced Cybersecurity Services Initiative

-Firms from half of the nation's 16 key industries, including wastewater and banking, have paid for special technology to join a Department of Homeland Security program that shares classified cyberthreat intelligence, NextGov reports. The voluntary program - known as the Enhanced Cybersecurity Services Initiative - was previously limited to defense contractors. As part of the ECSI, "cleared Internet service providers feed nonpublic government information about threats into the anti-malware systems of critical sector networks," Aliya Sternstein [writes](#). "As of July, only three industries - energy, communications and defense - were using the service, according to an unfavorable DHS inspector general audit."

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](tel:202-994-5613). cspri@gwu.edu

304 Staughton Hall
707 22nd St., NW

Washington DC, DC 20052