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

Proposition

Resolved: The government should never engage in the bulk collection of personal data for national security purposes.

Debaters

Lee Tien from the Electronic Frontier Foundation, Senior Staff Attorney and Adams Chair for Internet Rights

Chris Soghoian of the American Civil Liberties Union, Principal Technologist and a Senior Policy Analyst

Orin Kerr of GW Law, Professor

Paul Clark of Secure Methods LLC, President and CTO

March 23, 2015

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

High Noon Event: This Wednesday Cybersecurity Debate
Lunch provided

National Security and Cyber Surveillance: A Debate

Time: 12:00 PM - 2:00 PM
*11:45 AM (with lunch - see below for details); 12:00 PM(debate itself)

Location:
Jack Morton Auditorium
School of Media and Public Affairs
805 21st St NW
Washington, DC 20052

This debate is the fourth event in a University Seminar series on Internet freedom and governance.

The currently planned format of the debate itself will be that used by Intelligence Squared, where the "winner" is deemed to be the side that has

Events

See Upcoming Events at a Glance

Click here for detailed descriptions

Follow Us

Follow us on Twitter: @gwCSPRI

Follow CSPRI Director, Lance Hoffman: @lancehoffman1

Follow CSPRI Associate Director, Costis Toregas: @DrCostisToregas

changed the most minds.

See http://intelligencesquaredus.org/debates/past-debates/item/1190-mass-collection-of-u-s-phone-records-violates-the-fourth-amendment-- for a similar debate. Ours will be in a university setting, with a different proposition. It may focus on control-at-collection vs. control-at-use arguments, or other items, depending on where the debaters take us.

The debate proposition and list of debaters is located in the left hand column. For event registration (free), click **here.**

Cyber Security Policy News

China acknowledges existence of hackers
-A high-level Chinese military organization has for the first time formally acknowledged that the country's military and its intelligence community have specialized units for waging war on computer networks, reports The Daily Beast. China has long publicly denied it has teams of hackers deployed against other national networks, but in a recent publication the country's leaders appear to have tired of that charade,writes Shane Harris. "The acknowledgment could have political and diplomatic implications for China's relationship with the United States and other Western powers," Harris writes. "U.S. officials have spent years marshaling evidence of China's cyber capabilities and have been escalating efforts to stop cyber spying."

Indeed, the government's efforts to deter computer attacks against the United States are not working and it is time to consider boosting the military's cyber-offensive capability, the head of U.S. Cyber Command told Congress last week. That's according to The Washington Post, which quoted Admiral Mike Rogers as saying the government's mostly-defensive cybersecurity posture isn't exactly having a deterrent effect. "Rogers said that President Obama has not yet decided to delegate authority to him to deploy offensive tools," writes Ellen Nakashima. "When asked by Chairman John McCain (R-Ariz.) whether he agreed that the 'level of deterrence is not deterring,' Rogers said: 'That is true.'"

FBI's hacking power to expand
A judicial advisory panel last week quietly approved a rule change that will broaden the FBI's hacking authority despite fears raised by Google that the amended language represents a "monumental" constitutional concern, reports The National Journal. "Known as Rule 41, the existing provision generally allows judges to approve search warrants only for material within the

geographic bounds of their judicial district," Dustin Volz writes. "But the rule change, as requested by the department, would allow judges to grant warrants for remote searches of computers located outside their district or when the location is unknown."

Volz also covers an important development that could expand the government's power for cyber spying by default. The National Security Agency could be allowed to continue hoovering up American phone records indefinitely -- even if congressional authority for the spying program expires later this year. Also Volz writes, the legal underpinning of the NSA's bulk collection of U.S. call data resides in a provision of the post-9/11 USA Patriot Act that is scheduled to sunset on June 1. "The common understanding among lawmakers and the intelligence community is that the surveillance program will halt unless Congress reauthorizes Section 215 of the Patriot Act in some fashion," Volz wrote. But a passage buried on the last pages of an order from the Foreign Intelligence Surveillance Court declassified last week leaves open the door for the program-exposed publicly by Edward Snowden nearly two years ago-to continue even if lawmakers let Section 215 lapse."

FFIEC to update cybersecurity guidance

-The top banking regulatory agency revealed plans last week to update and supplement its cybersecurity guidance for banks. The Federal Financial Institutions Examination Council said the new guidelines for bank examiners were "to reflect rapidly evolving cyberthreats and vulnerabilities, with a focus on risk management and oversight; threat intelligence and collaboration; cybersecurity controls; external dependency management; and incident management and resilience." According to GovInfoSecurity, the FFIEC did not indicate when the new policies designed to help institutions address cybersecurity would be issued.

Facebook publishes new report on requests for user data

-Facebook has published its latest report on the requests it gets for user data from governments around the world, and while there's been a fall in requests from Western countries like the United States and Germany, there's been a rise in India, Turkey and Russia, reports Forbes. "The total number of requests has risen slightly to 35,051 from 34,946 from the first to the second half of 2014," writes Parmy Olsen. "Facebook also lists government requests to restrict or pull content, and said such request had risen by 11% to 9,707 pieces of content restricted."

The US wants "the right to be forgotten"

-Nearly nine in 10 U.S. voters want "the right to be forgotten" on the Internet, according to a new poll. The Hill writes that eighty-eight percent support a U.S. law that would let them petition companies like Google, Yahoo and Bing to remove certain personal information that appears in search results. Such a law would be similar to a measure already in place in Europe. Readers may recall that the previous University Seminar (prior to the one this Wednesday) dealt with this, featuring a lecture by Prof. Jeffrey Rosen. Details and some readings on the topic can be found here.

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