

# 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](#)

[CSPRI in the News](#)

[Cyber Security Policy News](#)

[Events](#)

## Quick Links

[About CSPRI](#)

[Contact Us](#)

[Newsletter Archive](#)

[Blog: The CSPRI Byte](#)

## CSPRI in the News

CSPRI Director Lance Hoffman was interviewed by the GW Hatchet about the Institute. Click [here](#) to read the story.

February 2, 2015

**Ten (10) Cyber security Events are scheduled in the Greater Washington Area in the next few weeks.**

## Cyber Security Policy News

### PCLOB Release

- An executive-branch privacy watchdog is renewing its call for President Obama to unilaterally end the National Security Agency's domestic phone records dragnet amid growing uncertainty over Congress's willingness to reform government surveillance, the National Journal reports. "The bipartisan Privacy and Civil Liberties Oversight Board issued a [progress report](#) Thursday charting the administration's efforts to comply with recommendations it made exactly a year ago to overhaul the NSA's surveillance apparatus," [writes](#) Dustin Volz. "That stern review last January also deemed the bulk collection of U.S. call data illegal and ineffective at countering terrorist plots- conclusions that prompted the board to urge its dissolution.

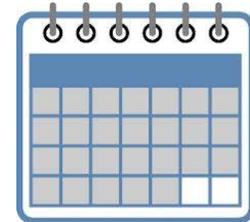
### Verizon supercookie update

-Days after [media reports](#) surfaced that Verizon was tracking subscribers with a special cookie file that customers could not remove, Verizon announced it would allow mobile subscribers to completely opt out of the online tracking tool that has raised privacy concerns among civil libertarians and Senate Democrats. "The company said it is working on the update and that a full opt-out to its so-called 'supercookie' would be available soon," [writes](#) Mario

## 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](#)

Trujillo. "The statement came a day after a group of Senate Democrats on the Commerce Committee sent a letter to the company demanding answers."

Follow CSPRI  
Research Scientist,  
Allan Friedman:  
[@allanfriedman](https://twitter.com/allanfriedman)



### US weapon programs flawed

-Most of the weapons programs in the United States contain security flaws, according to a report released by the US Defense Department's Director of Operational Test and Evaluation (DOT&E). "Nearly every U.S. weapons program tested in fiscal 2014 showed significant vulnerabilities to cyber attacks, including misconfigured, unpatched and outdated software," The New York Times [reports](#). "Michael Gilmore, director of operational test and evaluation (DOT&E), said program managers had worked to resolve problems discovered in previous years and security was improving, but this year's testing had revealed new vulnerabilities."

### Credit card metadata may be at risk

-Most credit card owners can be uniquely identified through the metadata included in just four credit card transactions per month, according to research by the Massachusetts Institute of Technology (MIT). "MIT researchers have reported that they do not need an individual's name, address, or credit card number, which are typically thought of as personal information, to identify people within a data set," [writes](#) Aimee Chanthadavong for ZDNet. "Instead, they say that using four vague pieces of information, such as the dates and locations of four purchases, are enough to identify 90 percent of the people in a data set recording three months of credit card transactions by 1.1 million users."

### Fitness wearables

-As the use of wearable fitness devices, health applications and interconnected medical devices expands, organizations need to take steps to protect the privacy and security of consumer data that these products collect, store and transmit, according to the Federal Trade Commission.

GovInfoSecurity [reports](#) on the [Internet of Things: Privacy & Security In a Connected World](#), which details the privacy and security concerns posed by Web-enabled consumer gadgets ranging from household appliances and automobiles, to health-monitoring and fitness devices.

#### 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](mailto:cspri@gwu.edu)  
304 Staughton Hall  
707 22nd St., NW  
Washington DC, DC 20052