

# 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](#)

March 30, 2015

**Five (5) Cyber security events are scheduled in the Greater Washington Area in the next few weeks.**

## National security and cybersurveillance debate

Prof. Lance Hoffman moderated a debate at GW on national security and cybersurveillance at GW on Wednesday, March 25. Watch the video [here](#).

### 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

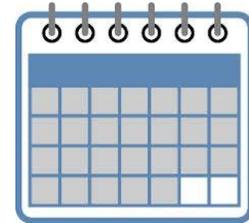
[Chris Soghoian](#) of the American Civil Liberties Union, Principal Technologist and a Senior Policy Analyst

[Orin Kerr](#) of GW Law, Professor

[Paul Clark](#) of Secure Methods LLC, President and CTO

## 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](#)



## Legislative Lowdown

- Legislation to create a national data security and breach notification standard moved forward last week over objections from Democratic lawmakers. Elise Viebeck at The Hill reports that the measure would require companies to maintain reasonable security practices and inform customers within 30 days if their data might have been stolen during a breach. Violations would subject companies to enforcement actions by the Federal Trade Commission (FTC). Read more [here](#).

-Also reporting for The Hill, Keith Laing [writes](#) that the Senate committee that oversees transportation considered a measure that would protect drivers' information that is collected by on-board event data recorders. The bill, which is known as the Driver Privacy Act, would stipulate that information collected by automobile data records belongs to the owner of the vehicle.

-The House Intelligence Committee last week unanimously approved a cybersecurity bill that would increase the sharing of computer data between government and the private sector, despite lingering concerns that the measure could allow for more government surveillance. Dustin Volz at National Journal [writes](#): "The House bill seeks to entice companies into voluntarily sharing more "cyberthreat indicators"-or computer data related to cybersecurity-with the government by offering them expanded liability protections for doing so. By sharing and analyzing greater amounts of data, backers of the bill say, government agencies and businesses can more effectively detect, minimize, and possibly even prevent debilitating hacks like the one that recently crippled Sony Pictures."

- A bill moving through the California state legislature that would require warrants to access all digital data has moved out of committee, Ars Technica [reports](#). "The California Electronic Communications Privacy Act" strives to protect citizens' privacy. Earlier versions of the bill have twice been vetoed by the governor.

## Cyber Security Policy News

-The United Nations top human rights body agreed on Thursday to appoint a special investigator to probe digital spying and violations of online privacy, according to Reuters. "Brazil and Germany spearheaded the resolution, which voiced deep concern over electronic surveillance and the interception of digital communications, as well as data collection by governments and private companies," [writes](#) Stephanie Nebehay. "The

Geneva forum, whose 47 members include the United States, adopted the text unanimously. During the debate, Russia's delegation criticized mass surveillance by the United States while Cuba took aim at 'certain Western powers.'"

-The FBI did not intentionally delete tips on how to protect the security of cellphones from its website, including one recommendation for using encryption security, National Journal reports. "The apparent scrubbing was [spotted](#) Thursday by the tech blog *Techdirt*," [writes](#) NJ's Dustin Volz. "The story suggested the FBI was surreptitiously removing the information because FBI Director James Comey has been publicly warning that new default encryption standards from Apple and Google could block law enforcement from accessing the data of criminal suspects."

-The Pentagon is having trouble putting its finger on exactly what it's getting for all the money it's spending on "cyber" projects, reports NextGov. "It all adds up to trouble planning cyber tactics, as adversarial nation states sharpen their own cyber know-how, according to budget analysts," [writes](#) Aliya Sternstein. "Earlier this month, in an initial Pentagon budget chart, it appeared 2015 CYBERCOM funding was labeled as a single line item, leading one to believe spending would sizably spike this year -- by 92 percent, when in fact it will slightly drop."

-Taiwan is seeking stronger ties with the U.S. government to combat a perceived threat from China, according to Reuters. "Taiwan wants to join a major anti-hacking drill conducted by the United States to strengthen cyber security ties with its staunchest ally, its vice premier said on Monday, a move which would help safeguard against constant targeting by hackers in rival China," the publication [reports](#). "Many hacks into Taiwan systems have been traced to sites belonging to China's People's Liberation Army, Vice Premier Simon Chang told Reuters in an interview, without elaborating on the locations."

-If you haven't yet created an account at [irs.gov](https://www.irs.gov), you may wish to take care of that before tax fraudsters do it for you. Security blogger Brian Krebs writes about the experience of a New York man who tried to get a copy of his tax transcript after learning that someone had filed a fraudulent tax refund in his name, only to find out that thieves had beat him to it. Read more [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](mailto:cspri@gwu.edu)*

*Tompkins Hall, Suite 106*

*725 23rd Street NW*

*Washington DC, DC 20052*