

# 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](#)

## Upcoming Events on Campus

### Breakfast and Business

**Cards: IT Security**

**Date:** February 24, 2015

*\*This event is open to GW alumni and current graduate students.*

For more information, click [here](#).

## February 23, 2015

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

## Oscar wins

**Cybersecurity is everywhere...even the 2015 Academy Awards!**

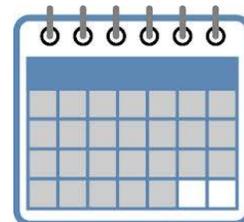
Cybersecurity isn't just a topic for consultants, policy writers, or computer scientists. It has now taken center stage, literally. This year at the Academy Awards, two security/privacy-related films took home prestigious titles.

[The Imitation Game](#) won the Oscar for Writing - Adapted Screenplay and [CitizenFour](#) won for Best Documentary Film.



## 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

-The Obama administration says that companies operating in the US must comply with US search warrants for data when that data is stored on overseas servers, writes Ars Technica. "The legislation, the [Law Enforcement Access to Data Stored Abroad](#) (PDF), is directed at a federal court's July ruling requiring Microsoft to turn over e-mails stored on its Irish servers to assist a Department of Justice drug investigation," [writes](#) David Kravets. "The bill would require companies based in the US to turn over data stored on its overseas servers only if the warrant targets a "US person." The legislation does not alter the law requiring US industry-when presented with a warrant-to hand over data stored on US servers no matter the target's nationality."

## Cyber Security Policy News

### **US and Iran: hostilities in cyberspace**

A [document](#) suggests that even while the high-stakes nuclear negotiations are playing out in Europe, day-to-day hostilities between the United States and Iran have moved decisively into cyberspace, [according to David Sanger in today's New York Times](#). "For the first time, the surveillance agency acknowledged that its attacks on Iran's nuclear infrastructure, a George W. Bush administration program, kicked off the cycle of retaliation and escalation that has come to mark the computer competition between the United States and Iran."

### **SIM cards: manufacturer hacked**

-Spies in the U.S. and United Kingdom hacked into the internal computer network of the largest manufacturer of SIM cards in the world, stealing encryption keys used to protect the privacy of cellphone communications across the globe, according to top-secret documents provided to *The Intercept* by National Security Agency whistleblower Edward Snowden. "The hack was perpetrated by a joint unit consisting of operatives from the NSA and its British counterpart Government Communications Headquarters, or GCHQ," the Intercept [reported](#) last week. "The breach, detailed in a secret 2010 GCHQ [document](#), gave the surveillance agencies the potential to secretly monitor a large portion of the world's cellular communications, including both voice and data."

### **Google comments on FBI's hacking plans**

-Google is coming out with some weighty words against the FBI's plans to expand its hacking activities, calling it a "monumental constitutional threat." The search giant submitted public comments earlier this week opposing a Justice

Department proposal that would grant judges more leeway in how they can approve search warrants for electronic data," [reports](#) Dustin Volz at the National Journal. "The push to change an arcane federal rule 'raises a number of monumental and highly complex constitutional, legal, and geopolitical concerns that should be left to Congress to decide," [wrote](#) Richard Salgado, Google's director for law enforcement and information security."

#### **Working to counter terrorism propaganda**

-The Obama administration is pursuing a plan to make it more difficult for extremist groups to spread their propaganda via social media. "Working with foreign nations and private companies, the administration will launch campaigns to counter terrorist groups' online propaganda, which have become a critical tool in their arsenal to spread their message and horrify people around the globe," [writes](#) Julian Hattem for The Hill. "In one effort, the government is organizing multiple 'technology camps' to work with companies and community groups 'to develop digital content that discredits violent extremist narratives and amplifies positive alternatives.'"

#### **State Department: email network still having problems**

-Three months after the State Department confirmed hackers breached its unclassified email system, the government still hasn't been able to evict them from the department's network, according to three people familiar with the investigation, The Wall Street Journal [reports](#).

Meanwhile, the hack has forced the State Department to replace some 30,000 network log-in fobs and digital tokens that employees had been using to access its systems remotely. As Aliya Sternstein [writes](#) for NextGov, "during the switchover, some State personnel said they were not able to access work outside the office for months."

#### **TurboTax Update**

-Two former security managers at Intuit, the makers of the popular online tax preparation software TurboTax, allege that the company has made millions of dollars knowingly processing state and federal tax returns filed by cybercriminals, [reports](#) KrebsOnSecurity. For its part, Intuit says it leads the industry in voluntarily reporting suspicious returns, and that ultimately it is up to the Internal Revenue Service to develop industry-wide requirements for tax preparation firms to follow in their fight against the multi-billion dollar problem of tax refund fraud.

#### 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:2029945613), [cspri@gwu.edu](mailto:cspri@gwu.edu)

Tompkins Hall, Suite 106

725 23rd Street NW

Washington DC, DC 20052