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

CSPRI in the News

On March 12, **CSPRI Director Prof. Lance Hoffman** joined Michael Daniel, White House Special Assistant to the President and Cybersecurity Coordinator; Bruce Heiman, K&L Gates; David O'Neil, Debevoise & Plimpton; and Amie Stepanovich, Access at a panel moderated by Daniel Castro of the Information Technology and Innovation Foundation on "Crypto Wars 2.0: How Should the U.S. Balance Privacy and National Security?".

An op-ed related to this by Prof. Hoffman appeared on the Christian Science Monitor website and a video of the event can be watched **here.**

March 16, 2015

Eleven (11) Cyber security events are scheduled in the Greater Washington Area in the next few weeks.

Event: March 25, 2015

National Security and Cyber Surveillance: A Debate

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 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 and won't have quite the production values they had, but also our proposition is different. It may focus on control-at-collection vs. control-at-use arguments, or other items, depending on where the debaters take us.

For event information, a list of panelists, and registration (free), click **here.**

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 Senate Intelligence Committee approved a billThursday seeking to increase the sharing of digital data between the government and private sector, marking the first serious move to upgrade the nation's cyber defenses since the crippling hack on Sony Pictures late last year, writes the National Journal. "In a closed-door meeting, the panel advanced 14-1 the Cybersecurity Information Sharing Act, which would provide expanded legal liability to companies so they more easily share digital data with the government-an arrangement the bill's backers say would help detect, prevent, and respond to cyber intrusions," reports Dustin Volz. Read more here.

-GovInfoSecurity has the lowdown on a proposal that would enact a national data breach disclosure law by usurping some 48 state breach disclosure laws already on the books. The story explains the tensions between privacy activists and the business community on a topic that has defied action for the better part of a decade.

Cyber Security Policy News

CIA involvement: cellphone data collection
-A Justice Department program employed to collect data from U.S. cellphones appears to have a silent partner: the Central Intelligence Agency (CIA). According to a story in The Wall Street Journal, the CIA played a role in helping the U.S. Marshals Service develop technology that imitates cellphone towers. "The program operates specially equipped planes that fly from five U.S. cities, with a flying range covering most of the U.S. population," The Journal reported. "Planes are equipped with devices-some past versions were dubbed "dirtboxes" by law-enforcement officials-that trick cellphones into reporting their unique registration information."

New surveillance tool comes with a nondisclosure agreement
Speaking of secret domestic surveillance activities, The New York Times carries a story about a powerful new surveillance tool being adopted by police departments across the country comes with an unusual requirement: to buy it, law enforcement officials must sign a nondisclosure agreement preventing them from saying almost anything about the technology. "Any disclosure about the technology, which tracks cellphones and is often called StingRay, could allow criminals and terrorists to circumvent it, the FBI has said in an affidavit," writes Matt Richtel for The Times. "But the tool is adopted in such secrecy that communities are not always sure what they are

buying or whether the technology could raise serious privacy concerns.

US industrial control systems: cyber attack target
-US industrial control systems were hit by cyber attacks at least 245 times over a 12-month period, the US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has revealed. The figure was included in a report by the ICS-CERT, which operates within the National Cybersecurity and Integration Center, a part of the Department of Homeland Security.

Clinton email scandal
-The scandal surrounding former State Dept. chief Hillary Clinton's exclusive use of private email services during her tenure won't go away, and isn't likely to do so anytime soon. According to The Hill, The Associated Press is filing a lawsuit to force the State Department to release emails and other documents from former Secretary of State Hillary Clinton. The Hill reports that the AP said the lawsuit to force the government to act came only after multiple requests under the Freedom of Information Act (FOIA) went unfulfilled.

OPM to up cybersecurity jobs
-The US federal government Office of Personnel Management (OPM) is making room for qualified individuals to fill up to 3,000 positions requiring "unique cyber security skills." However, as the SANS Internet Storm Center points out, it's unclear that there are that many qualified individuals available. "Everyone in the business says the same thing when they read this. 'Where are they going to find them?'" wrote SANS's Stephen Northcutt, in a weekly email newsletter. "Everyone is competing for the same people. And there is the problem of provable skills. Whoever is taking the lead on this truly important initiative has their hands full, and the authority expires December 31, 2015."

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