Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

The Weekly Newsletter of The George Washington University Cyber Security Policy and Research Institute

October 20, 2014

Twelve (12) Cyber security Events are scheduled in the Greater Washington Area in the few weeks.

In This Issue

Quick Links

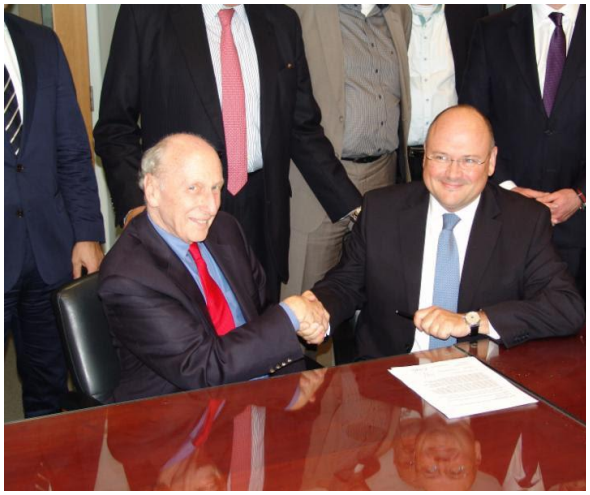
Upcoming CSPRI Event

Seminar event thisThursday, October 23rd(3-5 pm):

NET NEUTRALITY AROUND THE WORLD: Fundamental Right or Obstacle to Doing Business?

The event is free, but registration is

Announcements



Mr. Arne Schoenbohm, representing the Cyber-Security Council of Germany and Prof. Lance Hoffman (CSPRI director) shake on their signed agreement.

On October 17, GW's Cyber Security and Policy Research Institute (CSPRI) hosted a delegation of German industry and government representatives who met in the dean's conference room in Tompkins Hall with U.S. government officials and researchers to discuss shared cyber security issues and

Events

Click here for descriptions of the upcoming events!

Click the Calendar to See Upcoming Events at a Glance!

CSPRI in the News

In the Washington Post

Washington Post 'The Switch' writer Nancy Scola, extensively quoted Prof. Lance Hoffman, CSPRI Director, about a debate over encryption that Hoffman first participated in 20 years

required. Click **here** for the RSVP.

CSPRI, in the School of Engineering and Applied Science, has joined a cooperative effort with the School of Media and Public Affairs in the Columbian College of Arts and Sciences, the Institute for International Economic Policy in the Elliot School of International Affairs, and the Law School to present a seminar, Emerging Issues in Internet Freedom and Governance, that covers interrelated areas of international Internet policy that are prominent in public and scholarly debate and will shape the contours of the future global Internet. Running themes include the tensions between freedom and (cyber)security, privacy and publicity, and commercial development and the public good. The series events frame the underlying issues and address competing prescriptive measures, such as industry self-regulation and transparency reporting, as well as the technological implications and constraints. Click to see events, schedule, supporting background material, etc.

concerns. Present at the meeting were representatives of the U.S. State Department, the National Institutes of Standards and Technology, Rand Corporation, and the Information Technology Industry Council. The discussion topics included the new framework for cyber security promulgated by NIST and the concept of cyber insurance as a policy instrument to address cyber threats. At the end of the discussion, the head of the German delegation, Mr. Arne Schoenbohm, representing the Cyber-Security Council of Germany and Prof. Lance Hoffman (CSPRI director) signed an agreement to organize a long term, sustained program of academic exchanges, seminars and collaborative research intended to rebuild the trust between the two nations-traditional actors in a strong partnership in cyber security efforts-that recently has undergone challenges. The point of contact is CSPRI Associate Director Prof. Costis Toregas (toregas1@gwu.edu).

Legislative Lowdown

-Critics of the government's spy agencies are worried that Colorado's hotly contested Senate race could end the public career of one of their best allies in Congress, reports The Hill. "Sen. Mark Udall's (D-Colo.) possible defeat would leave a void in the Senate and on the powerful Intelligence Committee, civil liberties and anti-secrecy advocates fear,"writes Julian Hattem. "Udall has long been one of the Senate's biggest fighters against government secrecy, tough spying programs, the Guantanamo Bay detention facility and other issues important to civil libertarians."

Cyber Security Policy News

Chip and PIN technology for credit and debit cards
- President Obama last week signed an executive order intended to protect consumers' personal and financial information from hackers. According to the National Journal, the president mandated the installation of "chip and PIN technology" on new and existing government credit and debit cards starting next year. "The two-pronged upgrade aims to make payments to and from the federal government, for things like Social Security, more secure," writes Dustin Volz. "It is also designed to prompt the commercial sector to more quickly implement similar safeguards. So-called EMV chip technology is considered more secure than the magnetic strip found on the back of most payment cards because it makes creating counterfeit cards with stolen data more difficult. It is popular in many foreign countries, such as the United Kingdom, but has remained relatively rare in the United States, despite a recent string of gargantuan hacks at major retailers."

FBI Director clarifies statements given in *60 Minutes* interview
- FBI Director James Comey last week amended a public statement he made earlier in the week that the FBI never conducts electronic surveillance without a court order, NextGov reports. Comey had earlier given ago and that has been rekindled by remarks by FBI Director James Comey. Her column first appeared October 17.

Follow Us

Follow us on Twitter:
@gwCSPRI

Follow CSPRI Associate Director, Costis Toregas:
@DrCostisToregas

Follow CSPRI Research Scientist, Allan Friedman:
@allanfriedman

a speech warning that strengthened encryption measures in Apple and Google's new phones could lock out law enforcement from conducting the surveillance necessary to pursue criminal investigations and thwart terrorist plots. But as NextGov writes, Comey was asked to explain that answer in a question in a *60 Minutes* interview that aired on Sunday, where he claimed that the FBI never collects digital information without first obtaining judicial approval. "When I was asked that question, I gave an answer that I thought was fair and accurate, Comey told 60 Minutes. "And people gave me feedback afterward saying it was insufficiently lawyerly, it should have been longer, and what about the exceptions. And I think that's very fair feedback, and I wish I had thought of it in the moment."

POODLE vulnerability

-A newly disclosed vulnerability in an older but widely used technology for encrypting online Web site traffic has left browser makers and system administrators scrambling to implement changes to avoid the flaw. Dubbed "POODLE" by researchers (short for Padding Oracle On Downgraded Legacy Encryption"), Wired reports that it affects SSLv3 or version 3 of the Secure Sockets Layer protocol, which is used to encrypt traffic between a browser and a web site or between a user's email client and mail server. "It's not as serious as the recent Heartbleed and Shellshock vulnerabilities, but POODLE could allow an attacker to hijack and decrypt the session cookie that identifies you to a service like Twitter or Google, and then take over your accounts without needing your password," writes Wired's Kim Zetter.

Whisper app controversy

-Privacy advocates are anxious to see if federal regulators will go after Whisper, an app that promises anonymity but can allegedly track its users' movements, according to a story in The Guardian. The publication recently reported that Whisper keeps records of where users share their secrets, and that it stores, analyzes and, in some cases, shares with government agencies data on users' location, including those users that have opted-out of having their location information collected. Whisper's designers counter that the platform isn't really about concealing identity: It's about a complete absence of identity. "The concept around Whisper is removing the concept of identity altogether, so you're not as guarded," the company's co-founder and CEO, Michael Heyward, recently told Entrepreneur magazine. Heyward has referenced Whisper as the safest place on the Internet and paints the app as a secure place in which users should feel free to express their innermost feelings and confessions.

South Korea to replace national ID numbers due to cyber theft

-South Korea is facing the daunting prospect of having to replace 50 million national ID numbers that were

compromised in a recent cyber theft, the Associated Pressreports. The project could cost the government an estimated $650 million. "The issue came to a head after 20 million people including the president, Park Geun-hye, were victims of a data theft at three credit card companies," the AP writes. "Park acknowledged in January change was needed and ordered a study of possible options. A decision is due later this year."

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
304 Staughton Hall
707 22nd St., NW
Washington DC, DC 20052