Privacy and Security Are Not a Zero Sum Game

by Greg Nojeim [1]
February 11, 2011

The United States faces significant cybersecurity threats from state actors, from private actors motivated by financial greed, and from terrorists. Today, the House Armed Services Subcommittee on Emerging Threats and Capabilities held its first hearing on cybersecurity in this Congress.

This is an important subcommittee to watch. House Speaker John Boehner (R-OH) tasked its Chairman, Mac Thornberry (R-TX), with overseeing the process through which various Committees in the House will move cybersecurity legislation. Its ranking member, Jim Langevin (D-RI) is a Co-Chair of House Cybersecurity Caucus and a Co-Chair of the CSIS Commission on Cybersecurity for the 44th Presidency. I was privileged to testify at the hearing [2].

Members were interested in the role the Department of Defense should play in cybersecurity. Generally speaking, DOD entities – primarily the National Security Agency and the new Cybercommand – ought to focus their efforts on securing government military systems. However, they can also help the private sector secure its systems, and the Department of Homeland Security to secure civilian government systems, by sharing information and expertise. This is good for security, because DOD may have information -- including classified attack signatures -- that would help others defend their systems, and it is good for liberty because it diminishes pressure there would otherwise be to give DOD entities a leading role in cybersecurity outside of the .mil domain. In addition, DOD entities operate in a culture of secrecy – appropriate given their missions – that is inconsistent with the transparency that is needed to generate public trust and industry cooperation with cybersecurity measures for civilian systems.

I identified the Einstein intrusion detection and prevention system for federal networks as an area of needed oversight. The 3rd generation of Einstein is being tested, and operates on the network of an undisclosed ISP to protect the network of an undisclosed government agency, instead of operating on the network of the government agency. Thus, it is important to ensure that the system scans only communications to or from the government agency, to the exclusion of private-to-private communications.

Members were concerned about the possibility that a cybersecurity emergency could overwhelm the ability of a private sector critical infrastructure owner/operator to cope. They asked when/whether the military would have a directive role, and if so, what it would be.
I took this as an invitation to discuss the emergency authority some cybersecurity legislation would confer on the government to shut down or limit Internet traffic in a cybersecurity emergency. We think that the negatives that attend the grant of such authority outweigh the positives. A shut down is almost certain to have unintended collateral impact that could be significant, and the power to order a shut down could be used to coerce questionable conduct. It would create perverse incentives by discouraging operators of critical infrastructure systems from sharing cybersecurity information with the government out of fear it would be used to shut them down. Private operators who determine that shutting down a system would be advisable might hesitate to do so without a government order, and could lose precious time waiting to be ordered to shut down so they would less likely be held liable for the damage a shut down would cause others.

I also asked members to take a close look at any proposal to weaken cybersecurity by extending mandates like those in the Communications Assistance for Law Enforcement Act of 1994 to communications applications. CALEA now covers only telecommunications carriers, and broadband and interconnected VoIP services. Extending CALEA to communications applications to facilitate lawful surveillance would also create new vulnerabilities that would facilitate unlawful access by hackers, identity thieves and foreign entities.

Privacy and security are not a zero sum game. Measures intended to increase the security of

communications and transactions – such as identity and authentication requirements – need not threaten privacy and indeed may enhance it if properly deployed.

-
- Department of Defense
- cybersecurity
- CALEA

Links:
[1] https://www.cdt.org/personnel/greg-nojeim
[2] http://www.cdt.org/testimony/role-department-defense-cybersecurity