

## Cybersecurity: What's Next?

by [Greg Nojeim](#) [1]

November 19, 2009

*Everyone agrees:* cybersecurity is a big problem. Computer hackers are stealing government secrets and millions of dollars. Consumers' computers are being taken over unbeknownst to them and are being used to spread malicious computer code.

*Everyone agrees:* the status quo is untenable. Something has to be done about this problem, but there's no silver bullet. Cybersecurity solutions will involve consumers, communications and tech companies, and the government. With so many players, education and information sharing will be part of the solution.

*Everyone agrees, but only up to a point:* When the sleeves roll up and concrete ideas are put on the table, civil liberties warning signs begin to flash and privacy alarm bells begin to ring. That's what was happening at the [Senate Judiciary Committee](#) [2] hearing on cybersecurity on November 17 and scroll down to "Webcast Archives" on the right], at which I [testified](#) [3].

The hearing showed that tough questions about cybersecurity measures have yet to be resolved:

- What should be the role of the National Security Agency in securing civilian networks, and in particular, will it have a role that permits it to monitor private-to-private communications as a security measure?
- How can the government's legitimate right and responsibility to protect its own systems from computer attack be exercised without chilling the communications Americans have with their government and with minimal privacy impact?
- To what extent should current law change to permit the sharing of communications information for cybersecurity reasons?
- Will identity and authentication measures be deployed properly to promote privacy, or will they threaten it?

Based on the hearing, two things are clear: first, government agencies with significant cybersecurity responsibilities - the Department of Justice, the Department of Homeland Security, the National Security Administration - are working with the White House National Security Council to come up with cybersecurity legislation. Under pressure from Senator Whitehouse (D-RI), each administration witness agreed that the current legal structure in which they operate is not satisfactory, and the DOJ witness revealed that legislation is being discussed. The scope of legislative proposals and the time line for publicly announcing them have not yet been set.

Second, the open process that characterized the formulation of the White House Cyberspace Policy Review - the cybersecurity recommendations made to the President on May 29 by his homeland security and national security advisors - has not yet been carried over into the formulation of cybersecurity legislative proposals. While the White House eagerly sought the views of CDT and others during the cybersecurity review last spring, there has not yet been a consultation of which we are aware with privacy and civil liberties groups on the legislative proposals. This should concern every civil libertarian because what comes out of those discussions could have significant civil liberties implications.

This is not to say that legislation isn't needed. In fact, certain changes may very well be necessary, as CDT acknowledged to the Judiciary Committee. However, if we are ever to effectively address the cybersecurity problem, transparency and consultation are needed - with industry and the privacy and civil liberties communities -- about the problems that need to be addressed and the proposals for dealing with them. Any legislation should be narrowly focused on the problem at hand, and should not infringe unnecessarily on civil liberties or on the openness and innovation that

characterize the Internet.

The White House Cyberspace Policy Review, released in May, advised that, "... the Federal government should engage academia, civil liberties and privacy groups, advocates of open government, and consumers to ensure that government policy adequately considers the broad set of interests that they represent."

The White House needs to follow its own advice - starting sooner rather than later - as it formulates its cybersecurity legislative proposals.

- 
- [White House Cyberspace Policy Review](#)
- [NSA](#)
- [DHS](#)
- [cybersecurity](#)

Copyright © 2013 by Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

**Source URL:** <https://cdt.org/blogs/greg-nojeim/cybersecurity-whats-next>

#### Links:

[1] <https://cdt.org/personnel/greg-nojeim>

[2] <http://judiciary.senate.gov/>

[3] [http://cdt.org/files/pdfs/20091117\\_senate\\_cybersec\\_testimony.pdf](http://cdt.org/files/pdfs/20091117_senate_cybersec_testimony.pdf)