

Cybersecurity's 7-Step Plan for Internet Freedom

by [Greg Nojeim](#) [1]

March 28, 2012

Cybersecurity is important to all Internet users because it can make the Internet a safer place to shop, conduct business, and communicate with others.

However, pending cybersecurity bills include provisions that pose major civil liberties risks that must be addressed before any bill is enacted into law. This is urgent: the House is ready to take up legislation as soon as the week of April 23; after that, the Senate will act.[1](#)

Here are some "do's and don'ts," more fully explained in this [analysis](#) [2] for Senate cybersecurity legislation that preserves Internet privacy and freedom:

1. Don't Turn Cybersecurity Into a Backdoor Wiretapping Program. Information shared for cybersecurity reasons should be used for cybersecurity purposes, including enforcement of cybersecurity criminal laws. Instead, the Lieberman bill, S. 2105, permits the information to be turned over to law enforcement. The McCain bill, S. 2151, and the Rogers bill, H.R. 3523, are both worse because they permit it to be used for both law enforcement and national security reasons not related to cybersecurity. This turns cyber into a new surveillance program. Of the major bills introduced so far, only the Lungren bill, H.R. 3674, gets this right.

2. Don't Give the Keys To the Castle to the NSA. The super-secret National Security Agency is lobbying to get more access to private communications under a cybersecurity umbrella. Information is power, and NSA wants more of it, and may be building [space](#) [3] to store it. A military intelligence agency, NSA operates secretly for good reasons. But, it has abused secrecy before, engaging in years of warrantless wiretapping in the U.S. starting in 2001. Civilian control of cybersecurity helps promote transparency and accountability to the public for failure or abuse. Unfortunately, the McCain bill invites the NSA in, enticing companies to share with it ill-defined cyber threat information, and the Rogers bill has the same effect. The Lungren bill gets this right, too, putting DHS firmly in charge.

3. Don't Hide the Ball on NSA Role. Instead of specifying the federal agency that will take the lead on cybersecurity information sharing, the Lieberman bill punts: it tells DHS to decide, and empowers DHS to choose itself, NSA, or another agency. If DHS is to have the lead role, the bill should say so. It's the right call. To be fair, the McCain bill tries to hide the ball about whether NSA would assume a similar role, but Senator McCain has [plainly advocated](#) [4] giving NSA this role.

4. Don't Broadly Authorize Companies To Monitor their Customers. The Lieberman bill authorizes ISPs and other companies to monitor their information systems, and the computers of others who give permission, for "cybersecurity threats." Cybersecurity threats include "any action" that may result in unauthorized access to, theft of, or manipulation of data that is stored on or transiting any system, not just their own or that of their customer. Hold on! That's a lot to watch for: sharing a link to a file-sharing site may result in "unauthorized access" to information. So might forwarding an email. Sharing the password to your Gmail account is an "action" that may result in unauthorized access. This is very troubling, and it is unnecessary because current law gives companies the authority they need to monitor their networks to protect them. The Lungren bill in the House also authorizes monitoring, but only for a much more limited scope of genuine cyber threats to an ISP's network.

5. Don't Make Net Neutrality a Victim of Cybersecurity "Countermeasures". The FCC's Net Neutrality rules provide ample leeway for companies to engage in "reasonable network management" to ensure network security. But the Lieberman bill potentially goes further, giving companies an open-ended invitation to engage in countermeasures such as blocking and throttling even when it would otherwise violate the Net Neutrality rules or other law. Cybersecurity shouldn't

be allowed to function as an excuse for throttling lawful and non-malicious applications that happen to be bandwidth-intensive. The Lieberman bill would even permit ISPs to reach into their customers' computers to modify data packets if the consumer "lawfully authorizes" the countermeasure when she accepts the terms of service. The McCain bill also includes new monitoring and countermeasures authorities that are at least as disturbing because they are more vague.

6. Don't Authorize the Government To Seize the Family Home When Junior Violates Somebody's Terms of Service. The White House, the Senate Judiciary Committee and the McCain bill all increase the penalties for violating of the Computer Fraud and Abuse Act, the federal anti-hacking statute. The legislation would make CFAA violations a RICO predicate (thereby triggering treble damages), subject real property to civil forfeiture for CFAA violations, and create new mandatory minimums. But DOJ thinks that when you violate website, network or software terms of service, you violate the CFAA, and has prosecuted people for doing it. If the penalties for computer hacking are to be increased, at least [require](#) [5] that hacking occur. Mere violation of terms of service shouldn't trigger civil or criminal liability under the CFAA. The McCain and Senate Judiciary Committee bills get this mostly right, but DOJ is working hard persuade Congress to get this wrong.

7. Do Narrowly and Carefully Define the Cybersecurity Information that Can Be Shared. The Lieberman bill carefully lists specific categories of cyber threat indicators that companies can share and this is helpful. But it opens the door to misuse by saying that information that is merely "indicative" of one of those indicators can be shared. When it comes to cybersecurity information sharing, clarity is a virtue: cybersecurity threat indicators can be shared and other information cannot. And, confusion is a vice. Here is a paraphrase of the McCain bill's description of one category of information that can be shared for cybersecurity reasons: a private entity may share any information that would "foster situational awareness of the United States security posture" notwithstanding any law, if disclosure of such information is not otherwise prohibited by law. Huh? Can a company share the information if a privacy law protects it? In the post 9-11 intelligence mindset where it seems that every "dot" must be collected and connected, what information wouldn't foster situational awareness?

There you have it! Seven simple rules for increasing cybersecurity without damaging Internet freedom and privacy. Following these rules could help ensure that cybersecurity legislation does not trigger the same kind of upset that derailed the SOPA ("Stop On-Line Piracy Act") legislation last year.

1. [1](#). In the House, CDT supports the [Lungren](#) [6] bill and opposes the [Rogers](#) [7] bill.

- [Security & Surveillance](#)
- [monitoring](#)
- [cybersecurity](#)
- [countermeasures](#)
- [Congress](#)

The copyright © 2013 by the 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/2803cybersecuritys-8-step-plan-internet-freedom>

Links:

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

[2] <https://www.cdt.org/report/analysis-senate-cybersecurity-bills-2012>

[3] http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1

[4] <http://www.wired.com/threatlevel/2012/02/cybersecurity-act-of-2012/>

[5] <https://www.cdt.org/blogs/joshua-gruenspecht/wh-cybersecurity-proposal-cfaa-hack-goes-beyond-hackers>

[6] <https://www.cdt.org/blogs/greg-nojeim/22lungren-cybersecurity-bill-takes-careful-balanced-approach>

[7] <https://www.cdt.org/blogs/greg-nojeim/112cyber-intelligence-bill-threatens-privacy-and-civilian-control>