

Federal Authority Over the Internet? The Cybersecurity Act of 2009

by Jennifer Granick via Kismo - EFF Wednesday, Apr 15 2009, 10:50am

international / social/political / other press

There's a new bill working its way through Congress that is cause for some alarm: [the Cybersecurity Act of 2009](#), introduced by Senators Jay Rockefeller (D-WV) and Olympia Snowe (R-ME). The bill as it exists now risks giving the federal government [unprecedented power](#) over the Internet without necessarily improving security in the ways that matter most. It should be opposed or radically amended.

Essentially, the Act would federalize critical infrastructure security. Since many of our critical infrastructure systems (banks, telecommunications, energy) are in the hands of the private sector, the bill would create a major shift of power away from users and companies to the federal government. This is a potentially dangerous approach that favors the dramatic over the sober response.

One proposed provision gives the President unfettered authority to shut down Internet traffic in an emergency and disconnect critical infrastructure systems on national security grounds goes too far. Certainly there are times when a network owner must block harmful traffic, but the bill gives no guidance on when or how the President could responsibly pull the kill switch on privately-owned and operated networks.

Furthermore, the bill contains a particularly dangerous provision that could cripple privacy *and* security in one fell swoop:

The Secretary of Commerce— shall have access to all relevant data concerning (critical infrastructure) networks without regard to any provision of law, regulation, rule, or policy restricting such access...

In other words, the bill would give the Commerce Department absolute, non-emergency access to "all relevant data" without any privacy safeguards like standards or judicial review. The broad scope of this provision could eviscerate statutory protections for private information, such as the Electronic Communications Privacy Act, the Privacy Protection Act, or financial privacy regulations. Even worse, it isn't clear whether this provision would require systems to be designed to enable access, essentially a back door for the Secretary of Commerce that would also establish a primrose path for any bad guy to merrily skip down as well. If the drafters meant to create a clearinghouse for system vulnerability information along the lines of a US/CERT mailing list, that could be useful, but that's not what the bill's current language does.

A privacy threat still in the cocoon is the provision mandating a study of the feasibility of an identity management and authentication program with just a nod to "appropriate civil liberties and privacy protections." There's reason to fear that this type of study is just a precursor to proposals to limit online anonymity. But anonymity isn't inherently a security problem. What's "secure" depends on the goals of the system. Do you need authentication, accountability, confidentiality, data integrity? Each goal suggests a different security architecture, some totally compatible with anonymity,

privacy and civil liberties. In other words, no one “identity management and authentication program” is appropriate for all internet uses.

Whether the bill is amended or rejected, the question remains what kind of actions would help cybersecurity, and what role the federal government has to play. As security expert [Bruce Schneier](#) has [pointed out](#), the true causes of government cyber-insecurity are rather mundane:

GAO reports indicate that government problems include insufficient access controls, a lack of encryption where necessary, poor network management, failure to install patches, inadequate audit procedures, and incomplete or ineffective information security programs.

The Cybersecurity Act is an example of the kind of dramatic proposal that doesn't address the real problems of security, and can actually make matters worse by weakening existing privacy safeguards - as opposed to simpler, practical measures that create real security by encouraging better computer hygiene. We'll be watching this bill carefully to ensure that it doesn't pass in its present form.

Copyright applies.

<http://www.eff.org/deeplinks/2009/04/cybersecurity-act>

Cleaves Alternative News. <http://cleaves.lingama.net/news/story-1526.html>