CISPA Still Fundamentally Flawed

by Leslie Harris [1]
February 15, 2013

What a difference a year didn't make. On Wednesday, House Intelligence Committee Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger reintroduced the Cyber Intelligence Sharing and Protection Act, or CISPA, the same bill that passed the House [2] last April over the opposition [3] of civil liberties and Internet freedom groups and despite a Presidential veto threat [4].

Much has happened since last year's CISPA battle, including significant progress on a Senate cybersecurity bill [5] that had stronger privacy protections and the issuance just this week of an Executive Order [6] on cybersecurity that required privacy be protected in the very design of federal cybersecurity programs. And yet, CISPA has been reintroduced as it passed the House last Congress, still bearing the flaws [7] that gridlocked progress last year on the critical but difficult issue of information sharing.

CISPA's flaws are two-fold: First, the bill creates a sweeping cybersecurity exception to all of our hard won privacy protections and then encourages (through grants of immunity) companies to share private Internet communications and information directly with the NSA, a military intelligence agency that operates secretly with little public accountability. Second, it allows that private information, once it is in the hands of the military, to be used for purposes completely unrelated to cybersecurity.

We do need to figure out how to improve information sharing on cyberthreats among companies and between the government and the private sector. The new Executive Order should increase the flow of cyberthreat information from the government to the private sector. That is an important step forward. The next issues to be addressed – allowing companies to share information with each other and with the government – may require changes to current privacy laws, but those changes must be narrowly tailored.

Cybersecurity information sharing legislation should restrict the government from using cyberthreat information received from the private sector for non-cybersecurity purposes, and it should make the civilian-led Department of Homeland Security the focal point of cybersecurity efforts aimed at the private sector. Congress should not allow cybersecurity information sharing to become a back door wiretap and general intelligence collection tool. CDT has consistently argued that we can protect both cybersecurity and privacy, and we believe that is especially true of the information sharing issue [8].

-
- NSA
- cybersecurity
- CISPA

Copyright © 2013 by Center for Democracy & Technology.
The content on this website that originates with CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. Details.
Source URL: https://www.cdt.org/blogs/leslie-harris/1502cispa-still-fundamentally-flawed

Links:
[1] https://www.cdt.org/personnel/leslie-harris
[2] http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/HR624.pdf
[3] https://www.cdt.org/files/pdfs/Opposition-Letter-On-CISPA.pdf

[4] http://www.scribd.com/doc/91268009/White-House-issues-statement-against-CISPA
[5] http://www.hsgac.senate.gov/issues/cybersecurity
[6] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
[7] https://www.cdt.org/blogs/greg-nojeim/1804concerns-mount-over-unresolved-privacy-issues-cispa
[8] https://www.cdt.org/testimony/cybersecurity-innovative-solutions-challenging-problems