NETWORKWORLD

Stop Cyber Spying: Stop CISPA the New Enemy of the Internet

An Internet advocacy coalition launched Stop Cyber Spying Week, urging us to protest CISPA cybersecurity legislation which the House is set to vote on next week and has a decent shot of being passed. There's no time to delay adding your voice to the opposition if you care about privacy and civil liberties. OR you can stay silent and thereby endorse the government wiretapping and vaccuming up all your online communications.

By Ms. Smith on Wed, 04/18/12 - 11:16am.

We are half way through Stop Cyber Spying Week and there's no time to dawdle if you care about privacy and civil liberties, since the House is set to vote on the Cyber Intelligence Sharing and Protection Act (CISPA) [PDF] next week. Perhaps in part due to the rumble of growing protests about the "disturbing privacy dangers of CISPA," such as seen with the hashtags #CongressTMI and#CISPA, the Obama administration "blasted" CISPA by opposing any cybersecurity bill that violates citizens' privacy and civil liberties. Without explicitly saying "CISPA," the White House issued this statement:

> While information sharing legislation is an essential component of comprehensive legislation to address critical infrastructure risks, information sharing provisions must include robust safeguards to preserve the privacy and civil liberties of our citizens. Legislation without new authorities to address our nation's critical infrastructure vulnerabilities, or legislation that would sacrifice the privacy of our citizens in the name of security, will not meet our nation's urgent needs.

CISPA "would create a loophole in all existing privacy laws that would allow companies like Google and Facebook" to "pass your online communications *to the military*, just by claiming they were motivated by 'cybersecurity purposes.' Once the government has the information, the bill allows them to use it for any legal purpose other than regulation, not just for stopping cybersecurity threats,"explained the ACLU.

We all can see the need for some cybersecurity legislation, but we "cannot support overly broad legislation with no restrictions on government abuse." CDT President Leslie Harris said, "We need cybersecurity legislation, not surveillance legislation." A cybersecurity bill can make the Internet a safer place without jeopardizing Internet freedom and our civil liberties. Some of the CDT's do's and don'ts include great wisdom such as **Don't Turn Cybersecurity Into a Backdoor Wiretapping Program**; and **Don't Give the Keys To the Castle to the NSA**.

Microsoft, Facebook, AT&T, Verizon and others have sent letters supporting CISPA. Facebook defended CISPA, but denied the company intends to share users' sensitive personal information with the government. While Google is not on that list, Rep Mike Rogers told The Hill that Google is "supportive" of CISPA and "has been working behind the scenes with lawmakers."

CISPA is not SOPA as Jim Dempsey of The Center for Democracy and Technology (CDT) explained. The CISPA bill (H.R. 3523) was introduced in the US House of Representatives by Reps. Mike Rogers (D-MI) and C.A. "Dutch" Ruppersberger (D-MD). CISPA "is about government monitoring. [SOPA] is about the First amendment, [CISPA] is about the Fourth, but they both take a legitimate problem and try to tackle it with an overbroad solution," Dempsey explained. So US

News asked do you care more about the First or the Fourth amendment? Ummm hello? Constitution! Do we really have to pick and choose? I vote both!

The House Intelligence Committee launched a new Twitter account @HouseIntelComm specifically to spread misinformation, according to Techdirt. More misinformation is pouring out from Rep Mike Rogers. He tweeted about his bill "cementing privacy and civil liberties protections," but the revised version of the CISPA [PDF] does no such thing. The language is too vague and way too broad, and uses the word "notwithstanding" which basically would allow wiretaps.

The Cato Institute warned, that "a sysadmin with a vigilante streak reading ['cybersecurity systems']" could "include aggressive countermeasures, like spyware targeting suspected attackers...After all, 'notwithstanding any other provision of law' includes provisions of (say) the Computer Fraud and Abuse Act that would place such tactics out of bounds."

Despite the CISPA rewrite, it could still allow the NSA to hover up "all sorts of sensitive information like Internet use information and the contents of e-mails," ACLU legislative counsel Michelle Richardson told CNET. Furthermore the ACLU warned that the "notwithstanding" language left in the revised CISPA, "would trump wiretap laws, Web companies' privacy policies, gun laws, educational record laws, census data, medical records, and other statutes that protect information."

The EFF warned, "Yes, CISPA could allow companies to filter or block Internet traffic."

One of the scariest parts of CISPA is that the bill goes above and beyond information sharing. Its definitions allow for countermeasures to be taken by private entities, and we think these provisions are ripe for abuse. Indeed, the bill defines "cybersecurity purpose" as any threat related to safeguarding or protecting a network. As long as companies act in "good faith" to combat such a cybersecurity threat, they have leeway to protect against "efforts to degrade, disrupt, or destroy [a] system or network." This opens the door for ISPs and other companies to perform aggressive countermeasures like dropping or altering packets, so long as this is used as part of a scheme to identify cybersecurity threats. These countermeasures could put free speech in peril, and jeopardize the ordinary functioning of the Internet. This could also mean blocking websites, or disrupting privacy-enhancing technologies such as Tor. These countermeasures could even serve as a back door to enact policies unrelated to cybersecurity, such as disrupting p2p traffic.

It's hump day and we are half way through Stop Cyber Spying Week so there is no time to lose. CISPA has a decent shot at being passed. You could find your representative and your Rep's Twitter handle on the ACLU, or you could send an email to Congress. What you do online is *none* of the government's business and it doesn't get much easier to protest CISPA than with the new Congressional Twitter handle detection tool. The Twitter campaign, according to the EFF, is "because Congress is vacuuming up Too Much Information."

Show your congressperson the many things you do online - the personal, the mundane, whatever - so they can see just how much personal, unnecessary data could be vacuumed up as a result of the legislation's dangerously vague language. Use the hashtags #CongressTMI and #CISPA.

If you need a bit of inspiration, then check out some of these tweets. If you still need to understand more about what's wrong with CISPA, do not dally as clock is going tick tock and moving us closer to the House voting on CISPA next week.

Still undecided about making your voice heard? Read even more at Save The Internet, Avaaz, ACLU,CDT, EFF, The Constitution Project, Engine Advocacy, Access Now, Fight for the Future, Demand Progress, Free Press, Open Congress, Reporters Without Borders, Privacy Rights Clearinghouse,Techdirt, TechFreedom, Sunlight Foundation or any of the other civil liberties groups in the Internet advocacy coalition that is taking the fight to Twitter in order to oppose CISPA.