Written by **Raven Clabough** on April 26, 2012

Proposed Amendment to CISPA Adds More Controversy to Bill

Lee's amendment authorizes Napolitano to "acquire, intercept, retain" and "use" information that transits networks owned by the federal government or operated on its behalf by another carrier, such as Verizon. Napolitano has the power to do so if she claims that such surveillance would prevent "cybersecurity threats."

According to CNET News, the amendment is "so broad it trumps every existing privacy and surveillance law — to monitor all government networks, even ones operated by the FBI, White House, and the State Department."

A telecommunications attorney who wished to remain anonymous because of client sensitivity told CNET News that Lee's amendment was so broad in fact that it would include government contractors and university networks, and covers open wireless networks run by federal agencies and networks in government-provided housing.

Michelle Richardson, legislative counsel for the ACLU, explains: "Instead of having the private sector filter traffic [to] government Web sites for known or suspected signatures, they are just allowing DHS to do the tapping, filtering, and monitoring."

Ryan Radia of the Competitive Enterprise Institute believes the amendment could also permit the Department of Homeland Security to monitor the communications of the courts and of Congress, intercepting even tax returns sent to the IRS:

> While it appears that Rep. Jackson Lee sought to include several safeguards to limit DHS from improperly using and collecting information that flows on federal networks, those safeguards are essentially toothless. Under her amendment, the Secretary of Homeland Security need only "certif[y]" that the collection or interception of information by DHS complies with the various safeguards and limitations. But the Secretary of Homeland Security has the sole discretion to interpret the language of the safeguards as she sees fit. It appears that no judge or legislator can second-guess a Secretary's "certification" that a particular DHS information use accords with the bill's safeguards.

Lee's amendment seems to include all tech companies, including Apple, Yahoo, Facebook, McAfee, etc. "Cybersecurity services" is defined as widely as providing services that block "efforts to gain unauthorized access to a system."

It's not as if CISPA were not controversial enough before Lee's proposed amendment. Authored by Reps. Mike Rogers (R-Mich.) and Dutch Ruppersberger (D-Md.), CISPA would remove legal barriers that prevent companies from sharing information with one another with regard to cyber attacks. Supporters of CISPA claim that it seeks to give intelligence agencies and Internet companies more

incentives to share information with one another about security threats, such as hackers. But according to Talking Points Memo, there is more to the bill than that:

> The bill's critics contend that CISPA's terms are too broad, and could be interpreted in a way that removes important legal checks for when and how companies may turn over Web user information to the government.

For most critics, the underlying problem with CISPA is the section that states, "notwithstanding any other provision of law," which virtually allows CISPA to trump all existing federal, state, and criminal laws. The drafters of the bill claim that it's necessary in order to deal with threats from China and Russia and that it "protects privacy by prohibiting government from requiring private sector entities to provide information."

But organizations such as the Electronic Frontier Foundation, the American Library Association, the American Civil Liberties Union, and the Republican Liberty Caucus are not convinced.

Avaaz.org is organizing efforts to stop CISPA, circulating a petition entitled "Save the Internet from the US" that has nearly 800,000 signatures. That petition, addressed to members of the U.S. Congress, reads:

> As concerned global citizens, we urge you to immediately drop the Cyber Intelligence Sharing and Protection Act (CISPA). Our democracy and civil liberties are under threat from the excessive and unnecessary Internet surveillance powers it grants. The Internet is a crucial tool for people around the world to exchange ideas and work collectively to build the world we all want. We urge you to show true global leadership and do all you can to protect our Internet freedom.

Debate on the House floor begins today with a vote scheduled to take place on Friday. Opposition in the House has already begun to lay out criticism of the bill. Texas Republican and GOP presidential candidate Ron Paul compared the bill to "Big Brother writ large," while 18 House Democrats articulated their own privacy concerns pertaining to the bill in a letter. The letter raises three specific issues with CISPA: determining what information is shared, deciding who in the federal government has access to that information, and what will be done with that acquired information.

The letter concludes, "Without specific limitations, CISPA would, for the first time, grant non-civilian Federal agencies, such as the National Security Agency, unfettered access to information about Americans' Internet activities and allow those agencies to use that information for virtually any purpose."

Meanwhile, the White House has issued threats that it would veto CISPA because it fails to include "privacy confidentiality, and civil liberties safeguards." (See "related article" below.)

An email released by the White House states, "If H.R. 3523 were presented to the President, his senior advisors would recommend that he veto the bill."

However, most are unconvinced. Similar language came out of the White House in reference to the National Defense Authorization Act, famous for its indefinite detention provision, just before the President in fact signed the bill.

In fact, the email from the White House seems to reveal that the main issue the White House has with the bill is its failure to provide the DHS with enough power over the Internet.

"H.R. 3523 effectively treats domestic cybersecurity as an intelligence activity and thus, significantly departs from longstanding efforts to treat the Internet and cyberspace as civilian spheres. The

Administration believes that a civilian agency — the Department of Homeland Security — must have a central role in domestic cybersecurity, including for conducting and overseeing the exchange of cybersecurity information with the private sector and with sector-specific Federal agencies," states the email.

No need to worry, however. Rep. Jackson Lee seems to have that covered.

Related article: CISPA Assumes Too Much Trust in Government