reason hit & run
CONTINUOUS NEWS, VIEWS, AND ABUSE BY THE REASON STAFF

How the Newest Cybersecurity Bill Makes It Easier for the NSA to Spy On Your Online Activities

Peter Suderman | May 2, 2012

As the Internet helpfully reminds us, there are very few times when it is permissible to use the prefix "cyber." If you are William Gibson, it's fine. If you're typing a dirty IM, we'll let it pass. Notably absent from the list of exceptions? If you're a member of Congress trying to make it easier for government intelligence agencies to work with big tech corporations to spy on Americans' online activity. But that's exactly what a majority of House Republicans and 42 House Democrats did last week when theyvoted 248 to 168 to pass the Cyber Intelligence Sharing and Protection Act (CISPA), which would make it easier for Internet companies to provide information about their users and their networks to government intelligence agencies. And they passed it with minimal recognition of the very real privacy concerns critics have about the law.

The problem with CISPA, as with so many tech-sector laws, is that the legislative language is vague enough that it creates a big potential loophole — in this case for domestic spies to track individual activity. As CNet's Declan McCullagh explains, the law "wouldn't formally grant the NSA or Homeland security any additional surveillance authority," but it "would usher in a new era of information sharing between companies and government agencies — with limited oversight and privacy safeguards."

The idea behind CISPA is to facilitate corporate information sharing between government tech spies and the corporations who run online communications networks — which includes everything from web portals and social networking sites like Google and Facebook to Internet Service Providers like Comcast and Verizon.

The rationale for the law, as Cato Institute tech policy expert (and *Reason* contributing editor) Julian Sanchez points out, is that those companies have the best access to usage data that could be used to detect patterns that might represent potential threats. Currently, however, those companies are prohibited from sharing such information on an informal basis, in part to protect these highly regulated businesses from federal "nudges" intended to get them to "voluntarily" share information about network traffic or users. Under CISPA, tech companies

could more easily share “cyber threat information” with other other tech companies as well as with the government. They wouldn’t be forced to do so, but CISPA would override existing legal barriers to information sharing and collection.

If it’s all voluntary, is there really any reason to worry? Unfortunately, yes. One problem is that “threat information” is defined far too broadly. The language basically covers anything that anyone deems potentially a threat to any “system or network of a government or private entity,” including information “information directly pertaining to a vulnerability” in such a network. Information on attack patterns would be covered, but as Sanchez notes, depending on how you read the legislative language, “it might also include Julian Assange’s personal IM conversations (assuming he ever had an unencrypted one), or e-mails between security researchers.” Label any information a potential network threat, and it can be shared without the usual legal protections.

It's the potential to override those existing protections that's most worrying. As CNet's McCullaghwrites:

What sparked significant privacy worries is the section of CISPA that says "notwithstanding any other provision of law," companies may share information "with any other entity, including the federal government." It doesn't, however, require them to do so.

By including the word "notwithstanding," House Intelligence Committee Chairman Mike Rogers (R-Mich.) and ranking member Dutch Ruppersberger (D-Md.) intended to make CISPA trump all existing federal and state civil and criminal laws. (It's so broad that the non-partisan Congressional Research Service once warned (PDF) that using the term in legislation may "have unforeseen consequences for both existing and future laws.")

"Notwithstanding" would trump wiretap laws, Web companies' privacy policies, gun laws, educational record laws, census data, medical records, and other statutes that protect information, warns the ACLU's Richardson: "For cybersecurity purposes, all of those entities can turn over that information to the federal government."

If CISPA were enacted, "part of the problem is we don't know exactly what's going to happen," says Lee Tien, an attorney at the Electronic Frontier Foundation, which sued AT&T over the Bush administration's warrantless wiretapping program. "I worry that you can get a version of cybersecurity warrantless wiretapping out of this."

Numerous civil liberties, libertarian policy shops, and tech activist groups have come out against the bill: The American Civil Liberties Union warns that the bill “would create a loophole in all existing privacy laws, allowing companies to share Internet users' data with

the National Security Agency, part of the Department of Defense, and the biggest spy agency in the world — without any legal oversight." Tech Freedom's Berin Szoka has posted a number of strong criticisms of the bill, including worries that it would allow for the sort of coercion of corporations that the existing information gathering rules were designed to help prevent.

But as of now, most Internet businesses aren't speaking out about the bill. Unlike the last major tech proposals to hit Congress — the Internet-breaking anti-piracy bills SOPA and PIPA — CISPA is not widely opposed by major forces in the tech industry. Indeed, many are quietly supporting it. Which isn't entirely surprising: the law facilitates sharing between tech industry players, who would presumably like to be able to more easily access information from their peers and competitors, as it does between tech companies and government authorities. But as of yesterday, at least one notable tech has come out in explicit opposition to the bill: Mozilla, maker of the browser Firefox, told *Forbes*that CISPA "infringes on our privacy, includes vague definitions of cybersecurity, and grants immunities to companies and government that are too broad around information misuse. We hope the Senate takes the time to fully and openly consider these issues with stakeholder input before moving forward with this legislation." Sorry, Congress. It's still not OK to say cyber.