New American

Written by C. Mitchell Shaw on October 30, 2015

CISA Passes Senate, Threatens Liberty and Privacy

On Tuesday, the Senate passed the Cybersecurity Information Sharing Act (CISA) by a vote of 74-21. The bill, which is a bipartisan effort sponsored by both Dianne Feinstein (D-Calif.) and Richard Burr (R-N.C.), is aimed at "improv[ing] cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes." It's those "other purposes" that have the tech industry and the internet community worried. A surveillance bill by any other name is still as dangerous to liberty.

What makes the Cybersecurity Information Sharing Act a surveillance bill is the fact that the bill creates a way for companies to share information with the federal government and its myriad three-letter agencies about cyberattacks and threats of cyberattacks. That information would also include personal data about the customers, including names, addresses, what services they use, how they use them, when they use them, and more. If the company in question is your Internet Service Provider or mobile service provider, that information could include your browsing history and call logs.

In other words, just as more and more Americans are demanding that the federal government reform its surveillance programs, along comes CISA claiming to protect America's networks and conveniently providing another way for government to collect data on citizens. To make matters even worse, the bill does not address the real issues that threaten America's networks. CISA, in a play of smoke and mirrors, promises security it can't deliver and threatens to take away liberty and privacy. As Electronic Frontier Foundation (EFF) legislative analyst Mark Jaycox put it,

> The bill is fundamentally flawed due to its broad immunity clauses, vague definitions, and aggressive spying authorities. The bill now moves to a conference committee despite its inability to address problems that caused recent highly publicized computer data breaches, like unencrypted files, poor computer architecture, un-updated servers, and employees (or contractors) clicking malware links.
>
> The conference committee between the House of Representatives and the Senate will determine the bill's final language. But no amount of changes in conference could fix the fact that CISA doesn't address the real cybersecurity problems that caused computer data breaches like Target and the U.S. Office of Personnel Management (OPM).

The New American reported on CISA back in September and listed the OPM hack along with several others as examples of federal ineptitude and failure. In some cyberattacks that the federal government failed to prevent — and sometimes failed to detect — America's infrastructure and national security were jeopardized. The federal government's failure to secure America's networks should not serve as reason or justification for granting itself even broader, deeper authority to do what it has no business doing under the guise of trying to do something it has shown itself inept at.

Rather than take responsibility for the failure of his administration, President Obama pointed to the escalating danger of cyberattacks and the damage done by them as he laid the foundation for passing bills such as CISA. In February he said, "there's only one way to defend America from these cyber-threats — and that is from government and industry working together." Ironically, he made these remarks as the OPM hack was ongoing and unknown to him or those he appointed to guard those systems.

Many of the problems facing America's digital infrastructure are directly related to the surveillance culture fostered by the federal government. As this writer said in a previous article:

> Much of the common thread connecting all these events is a culture of surveillance that weakens computer security. When security holes are allowed to exist so that governments and corporations have an easier means of spying on people, hackers have a much easier time hacking. Instead of taking the advice of experts in the field of computer security, Obama and his allies in government have chipped away at privacy and liberty to continue perpetuating that surveillance culture.

CISA is another huge step in the fostering of that surveillance culture. It has been nearly six years in the making and has been defeated in other iterations. It has been opposed by the tech industry, academia, civil-liberty organizations, and concerned citizens. It's back for another round not because it is needed, but because the forces at work in Washington pushing the surveillance culture never give up.

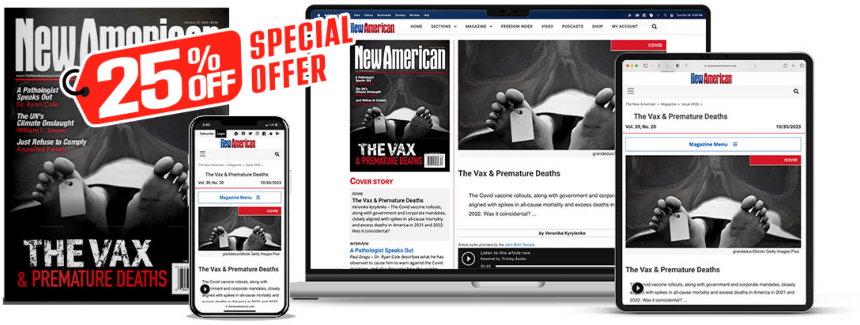
As EFF put it,

> The passage of CISA reflects the misunderstanding many lawmakers have about technology and security. Computer security engineers were against it. Academics were against it. Technology companies, including some of Silicon Valley's biggest like Twitter and Salesforce, were against it. Civil society organizations were against it. And constituents sent over 1 million faxes opposing CISA to Senators.

If, as EFF says, many lawmakers badly misunderstand technology and security, it may be well to listen to the people and companies that do understand technology and security. They all seem to have one thing in common: distrust of the Cybersecurity Information Sharing Act. A quick look at technology news sources reveals a pattern. They are all opposed to this bill. EFF, PCWorld, Wired, ZDNet, the *Guardian*, Slashdot, InfoWorld, NetworkWorld, Gizmodo, TechDirt, and others have all written of the dangers and general worthlessness of CISA. The list of technology news sources in favor of CISA is empty.

It is telling that experts in the field who typically enjoy spirited disagreement in everything from which smartphone or operating system is best, to the best way to backup and secure your data are all in agreement on this one thing. CISA is dangerous. It is — or at least will be used as — a surveillance bill. It will not protect America's networks, but it will provide the surveillance state an easier path to spying on Americans.

The House and Senate versions of this bill are not identical, so the differences still need to be ironed out before it can go to President Obama for his signature. There may still be hope of defeating CISA, if enough Americans pressure their representatives to scuttle the committee negotiations on getting the versions of this bill together. If not, and CISA becomes law, the surveillance culture will be codified into law and gain the appearance of legitimacy. That will make it much harder to dismantle the apparatus that has been put into place to spy on all of us.


25% OFF
SPECIAL OFFER
New American
THE VAX
& PREMATURE DEATHS
The Vax & Premature Deaths