Written by **Joe Wolverton, II, J.D.** on July 16, 2014

Senate Moves Closer to Seizing Control of Cyberspace

Just when you thought it was safe to get back on the Internet.

Tuesday, the Senate Select Committee passed the Cyber Information Security Act (CISA) by a vote of 12-3. This clears another hurdle in the path toward consideration by the body of the Senate.

CISA is in large part a substantially similar redux of other Internet-security bills that have been knocked around by Congress over the years. Last year, for example, a controversial cousin of CISA called the Cyber Information Sharing and Protection Act (CISPA) made it through the House of Representatives. It couldn't survive Senate scrutiny, however, and died amid allegations of privacy privations.

"The Cybersecurity Information Sharing Act (CISA)," reports Julian Hattem from *The Hill*, "makes it possible for companies and government agencies to share information about possible hackers and security weaknesses with each other, which advocates say is critical to make sure that blind spots aren't left untended for long."

{modulepos inner_text_ad}

One of the new bill's sponsors, Senate Intelligence Chair Dianne Feinstein (D-Calif.), believes that the measure would facilitate the effort of government and business to combat cyber-attacks by easing the exchange of critical data between the two entities.

VPN Creative reports that Feinstein said, "Every week, we hear about the theft of personal information from retailers and trade secrets from innovative businesses, as well as ongoing efforts by foreign nations to hack government networks … this bill is an important step toward curbing these dangerous cyber-attacks."

Privacy groups, however, know a government power grab when they see one.

After the bill passed out of committee, the Electronic Frontier Foundation (EFF) joined a group of 35 civil society organizations, companies, and security experts that sent a letter appealing to President Obama to veto CISA (S. 2588). The letter states:

> CISA fails to offer a comprehensive solution to cybersecurity threats. Further, the bill contains inadequate protections for privacy and civil liberties. Accordingly, we request that you promptly pledge to veto CISA. We also request that you issue a similar veto threat for any future legislation that takes a similar approach on information sharing. A robust approach to cybersecurity is necessary to protect the security of the internet and those who use it.

The letter goes on to point out that this latest incarnation of an Internet control bill makes little more

than "cosmetic changes to CISPA":

> CISA presents many of the same problems the Administration previously identified with CISPA in its veto threat. Privacy experts have pointed out how CISA would damage the privacy and civil liberties of users. Language in CISA, like CISPA, also bypasses the Administration's previously stated preference of having a civilian agency lead U.S. cybersecurity efforts in favor of automatic and simultaneous transfer of cybersecurity information to U.S. intelligence agencies, like the National Security Agency.

In a blog post announcing its contribution to the letter, EFF says of CISA:

> The bill fails to provide privacy protections for Internet users and allows information sharing in a wide variety of circumstances that could potentially harm journalists and whistleblowers. Like its previous iterations, it also contains overbroad immunity from lawsuits for corporations that share information. As the letter points out, it even contains "a broad new categorical exemption from disclosure under the Freedom of Information Act, the first since the Act's passage in 1966."

This is similar to the group's criticism of CISPA. In 2013, EFF said that the data the government is targeting with CISPA included medical records, credit reports, and most other "personally identifiable information" that might be caught in a cybersecurity net.

As pointed out above, the National Security Agency (NSA) is the primary beneficiary of all this data mining masquerading as cybersecurity.

Agents of this domestic surveillance mammoth would need no warrant before approaching Internet companies with requests for their customers' otherwise private information.

Regarding CISA, EFF claims it "jeopardizes the foundation of cybersecurity by improperly pitting human rights against security."

The signatories to the letter to the president urging him to veto CISA recommend adoption of a bill that "would both defend and extend civil liberties and the right to privacy of users globally."

Defense of civil liberty — even in cyberspace — is crucial, especially in light of President Obama's insistence that "the cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cybersecurity."

As is the case with CISA and so many other federal programs that are steadily and stealthily chipping away at our civil liberties that are the very foundation of our Republic, the will in Washington is to place every aspect of the lives of every American under the close watch of the federal government.

Accordingly, CISA, despite its many unconstitutional provisions, seems tailored this time to garner just enough support in Congress to actually make it to the president's desk.

And, contrary to President Obama's declaration that American prosperity depends on cybersecurity, friends of freedom know that the perpetuation of our Republic and the rights we enjoy depends on a return to first principles of liberty and a fearless defense of the Constitution that stands as sentinel of the natural rights granted to all men by their Creator.

For now, government monitoring of the Internet as authorized by CISA seems rejuvenated while Internet privacy slouches closer to death.

Joe A. Wolverton, II, J.D. is a correspondent for The New American *and travels nationwide speaking on*

nullification, the Second Amendment, the surveillance state, and other constitutional issues. Follow him on Twitter @TNAJoeWolverton and he can be reached at jwolverton@thenewamerican.com.