JUSTIN AMASH
THIRD DISTRICT OF MICHIGAN

OVERSIGHT AND GOVERNMENT REFORM COMMITTEE
SUBCOMMITTEE ON TRANSPORTATION AND PUBLIC ASSETS

JOINT ECONOMIC COMMITTEE

Congress of the United States
House of Representatives
Washington, DC 20515

WASHINGTON OFFICE
114 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-3831

DISTRICT OFFICES
110 MICHIGAN STREET NW, SUITE 460
GRAND RAPIDS, MI 49503
(616) 451-8383

70 WEST MICHIGAN AVENUE, SUITE 212
BATTLE CREEK, MI 49017
(269) 205-3823

December 17, 2015

Oppose Omnibus to Stop Anti-Privacy Cyber Bill

Dear Colleague,

On Wednesday afternoon, the chairman and ranking member of the House Permanent Select Committee on Intelligence (HPSCI) distributed a myth-fact sheet about the Cybersecurity Act of 2015—legislation that was negotiated in secret by a handful of members and then tucked into the omnibus appropriations bill. Their sheet contains inaccurate and misleading information. This cyber bill is the worst anti-privacy legislation since the USA PATRIOT Act.

Here are the real myths and facts.

MYTH #1:

The purpose of this cyber bill is not government surveillance.

FACT #1:

- ✓ **Security experts and systems administrators—including those at Amazon, Mozilla, and Twitter—agree that they do not need new legal authorities to help protect their systems from cyber attacks.** Companies already can, and do, share technical information pertaining to an attack with other companies while still complying with relevant privacy laws.
- ✓ **The bill encourages companies to share far more information than is necessary for simply detecting and mitigating cyber threats.** The bill authorizes companies to share "cyber threat indicators" about "cybersecurity threats" with the federal government and each other—notwithstanding any privacy and consumer protection laws that might otherwise protect such information—with the assurance that they will not be held liable for contract violations, disclosing user information, or inappropriately monitoring users' activities or content. The bill's terms are defined so broadly as to authorize the sharing of an unnecessarily wide range of information, including an excessive amount of users' personal, private data. There are no limits on the type of information that can be shared, which could include your private online communications.
- ✓ **The bill allows the government to use the information it receives for purposes completely unrelated to cybersecurity.** A bill that intends only to increase the sharing of actionable cyber threat information should limit the uses of that information to cybersecurity purposes. The cyber legislation that passed the House with the most support earlier this year included just such a restriction. This new bill allows the government to use the information shared with it by the private sector for numerous purposes unrelated to cybersecurity, calling into serious question proponents' claims about the bill's intentions.

MYTH #2:

The bill does not permit surveillance for law enforcement or other purposes by the government once the information is shared by the private sector.

FACT #2:

- ✓ **Nothing in the bill prohibits the government from searching the "indicators" it receives from private companies for information about specific individuals or for evidence of illicit activity.** Previous versions of cyber legislation in the House have included explicit prohibitions on using shared cyber threat information for surveillance purposes. This new bill includes no such restriction. HPSCI claims that because surveillance isn't explicitly *authorized* in the bill, the federal government will be unable to use the information as a surveillance tool. This is false.
- ✓ **The bill expressly permits the government to use the information it receives to respond to, investigate, and prosecute activities completely unrelated to cybersecurity**, including threats of serious bodily harm or economic harm, computer fraud, trade secrets violations, and several other criminal violations that have nothing to do with cyber attacks. These are serious crimes, but they should not be exempt from constitutional due process protections. This bill allows the government to search information it receives as "cyber threat indicators" for evidence of such crimes and to use that evidence to launch criminal investigations. In other words, the government may search your private data without a warrant and use that information against you.

MYTH #3:

The bill includes meaningful requirements that companies "scrub" personally identifiable information (PII) from cyber threat information before sharing.

FACT #3:

- ✓ **The bill permits broad sharing of personal information, including information stolen by hackers, and incentivizes companies to adopt lazy processes that permit the flow of your personal data to the government.** The bill asks only that a company remove information it "***knows*** *at the time of sharing*" to be personal information unrelated to a cyber threat. As long as the company doesn't ***know for a fact*** that it is private information unrelated to a threat, it's free to share it. Under this system, companies will naturally be inclined to overshare. And the bill provides these companies protection from liability for such sharing, even in cases of gross negligence.

MYTH #4:

The bill prevents consumers' personal, private information from being shared directly with the military or NSA.

FACT #4:

- ✓ **Although the bill establishes the government's primary sharing portal within the Department of Homeland Security (DHS), it requires DHS to establish processes to**

share the information it receives with other federal agencies—including intelligence agencies—automatically and **in real time.** There is no difference between sharing personal, private information directly with the NSA and sharing this information with DHS if DHS must then share the information with the NSA instantaneously. The information also will be shared automatically with the Departments of Defense, Commerce, Energy, Justice, and the Treasury, ensuring your personal, private data will end up in the hands of the FBI, the DEA, and the IRS.

- ✓ **The bill permits the president to designate another non-DoD federal entity—such as the FBI—to develop an alternative sharing portal a mere three months after the bill is enacted.**

MYTH #5:

The bill does not provide companies complete liability protection when their actions are grossly negligent or harm innocent third parties.

FACT #5:

- ✓ **Unlike previous versions of cyber legislation, this bill includes no exemptions to the liability waiver for gross negligence or willful misconduct. Under this bill, companies may overshare their users' personal, private information with complete immunity.**

The omnibus's Cybersecurity Act of 2015 is modeled after the Senate's Cyber Information Sharing Act (CISA), which industry leaders across the political spectrum have panned as dangerous to privacy and security. Make no mistake: This omnibus includes the worst anti-privacy legislation to come before the House since the USA PATRIOT Act. I urge my colleagues to join me in opposing this dangerous measure that expands unconstitutional surveillance of all Americans.

Sincerely,

/s/

Justin Amash