Cybersecurity...or Cyber-Surveillance?
The Cybersecurity Information Sharing Act (CISA) Will Vastly Increase Government Access to Americans’ Data

Since the National Security Agency’s mass surveillance of Americans was first revealed two years ago, many members of Congress in both parties have been pushing for reform of the legal authorities that the NSA’s data dragnets rely on.

However, instead of prioritizing the surveillance reform that Americans have been demanding, the Senate is considering the Cybersecurity Information Sharing Act of 2015 (CISA, S. 754), a bill that would increase intelligence agencies access to our personal data.

CISA Would:

- **Increase government access to innocent Americans’ personal data** by authorizing companies to share vaguely-defined “cyber threat indicators” that could include private communications content and sensitive, personally identifiable information, even when that data is unnecessary to identify or respond to a threat;
- **Enhance the NSA’s access to Americans’ private information and undermine civilian control of domestic cybersecurity** by allowing companies to share directly with the NSA, and requiring that all information shared with other federal agencies be immediately and indiscriminately shared with NSA;
- **Undermine Americans’ rights to privacy and due process** by allowing the FBI and other federal, state, and local law enforcement agencies to use information they receive for investigations that have nothing to do with cybersecurity; and
- **Permit companies to monitor all of Americans’ online communications and activities** by authorizing companies to look for threats to any network anywhere.

To Protect Americans’ Privacy and Civil Liberties, Vote “NO” on Cybersecurity Information Sharing Bills That Fail To:

- **Clearly define and limit what information can be shared with the government to technical indicators of threats that appear likely to cause harm;**
- **Require companies to remove personally identifiable information** unless it is necessary for identifying or responding to a cyber threat;
- **Restrict NSA access to information that contains personally identifiable information,** unless it pertains to a significant cyber threat;
- **Prohibit law enforcement from using information to investigate or prosecute crimes that are unrelated to cybersecurity;** and
- **Limit the authority for companies to monitor Americans’ communications where necessary to identify and protect against threats to one’s own network.**

FOR MORE INFORMATION, CONTACT ROBYN GREENE, POLICY COUNSEL, NEW AMERICA’S OPEN TECHNOLOGY INSTITUTE at greene@opentechinstitute.org.