By December of this year, Congress will have to vote on a controversial Internet spying authority. With this vote looming, lawmakers must decide whether to protect their constituents' privacy and defend the Fourth Amendment.

What is Section 702?

Section 702, created by the FISA Amendments Act, is ostensibly aimed at collecting foreign intelligence information from foreign persons located outside the United States. But Section 702 programs routinely sweep up millions of innocent Americans' emails, text messages, phone calls, and other online communications—all without a warrant. Despite repeated requests from lawmakers, Congress has yet to receive a promised report on how many Americans' communications are collected under Section 702. It is irresponsible for Congress to consider reauthorizing this surveillance authority without a complete accounting of the impact this surveillance has on Americans' privacy.

PRISM and Upstream

Section 702 covers at least two surveillance programs that became household names in the wake of the 2013 leaks from former government contractor Edward Snowden: PRISM and Upstream.

PRISM allows intelligence agencies to force tech companies like Google and Facebook to turn over users' Internet communications if those communications are to or from foreigners located overseas that the government has identified as foreign intelligence targets. The government then bars the companies from notifying their customers that their data has been released to the government.

In contrast, under Upstream the NSA directly taps into the Internet backbone—the network of high-capacity, long-distance fiber-optic cables owned by companies like AT&T and Verizon—then copies and searches the traffic on those cables. The NSA then scans that traffic to see if it contains tasked "selectors" or identifiers that the NSA has determined are related to foreign intelligence targets. Although selectors are often specific, like an email address or phone number, selectors can also be quite broad, like domain names.

How Section 702 impacts Americans

The intelligence community obtains billions of communications each year under Section 702, and the communications of Americans are routinely—and intentionally—swept up as part of process. Whenever an American communicates with an individual targeted for surveillance under Section 702, that American's communications with the target are intercepted and stored in intelligence community databases. Section 702 "targets" are not limited to terrorists or foreign government officials, though. Instead, agencies can "target" any foreign person or entity that is believed to posses "foreign

intelligence information," a group that potentially includes journalists, human rights advocates, foreign governments, and foreign companies. Americans' communications with these targets are nevertheless intentionally acquired and retained—what the government refers to as "incidental surveillance."

Once Americans' communications are collected, they are then stored in government databases. The FBI routinely searches through this data when looking into criminal cases, even those that raise no national security or foreign intelligence concerns. In other words, because of Section 702 surveillance, the FBI can easily get around the standard warrant requirement for searching Americans' communications. The House has voted twice since 2014 to close this "backdoor search loophole" by requiring these agencies to obtain a warrant before they can search for information about Americans in communications collected under 702.

Additionally, Upstream surveillance, itself, poses unique threats to Americans' privacy, because it allows the NSA direct access to the fiber-optic cables transmitting millions of Americans' communications. Although the NSA attempts to filter out wholly domestic communications from its collection, the technique is inherently imprecise and the NSA has consistently violated court-imposed restrictions on its upstream collection. These repeated violations recently pushed the NSA to voluntarily end a particularly controversial aspect of upstream—so-called "about" surveillance. Congress should codify this prohibition on "about" searches to ensure NSA does not restart the practice.

Support for ending this warrantless surveillance of Americans

U.S. tech companies have joined lawmakers in opposing this warrantless surveillance. In a letter earlier this year, the Reform Government Surveillance coalition urged congressional leadership to reform Section 702 to "enhance transparency, provide greater programmatic oversight, and strengthen protection of sensitive personal data." Specifically, the group pointed to limiting the information collected under Section 702 and requiring judicial oversight before the intelligence community can search through information collected under Section 702 for Americans' communications. The Internet Infrastructure Coalition called reform "necessary to restore confidence in internet companies, preserve the vitality of the free and open internet, and preserve the U.S. innovation economy" and warned of the "grave economic consequences" to U.S. companies if Congress fails to adequately reform Section 702 surveillance.

There is also mounting pressure from constituents to rein in warrantless Internet surveillance. Since Congress passed a set of modest reforms concerning phone record surveillance in 2015, over 500,000 people have signed a public petition[1] urging Congress to enact reforms to make clear that blanket surveillance of Internet activity and phone records of any person residing in the U.S. is prohibited by law and that violations can be reviewed in court.

[1] https://optin.stopwatching.us/?r=eff