

Section 702's Excessive Scope Yields Mass Surveillance: Foreign Intelligence Information, PRISM, and Upstream Collection

When Congress debated and passed the FISA Amendments Act of 2008, it was with the idea that this surveillance authority would help investigate and prevent terrorism and espionage. For this reason, Congress authorized the NSA to collect Americans' communications with foreigners with less judicial oversight, and under a standard that falls far short of the probable cause requirement under the Fourth Amendment. However, the NSA uses this authority to surveil communications that go well beyond the national security purpose of the law.

Section 702 surveillance falls into two categories of programmatic surveillance: PRISM and Upstream Collection. The surveillance targets individuals abroad who are in contact with Americans. Together, these two programs enable the NSA to incidentally sweep up Americans' communications at a scale much larger than the public and Congress ever conceived. For example, in 2013, the NSA monitored [89,138](#) targets pursuant to Section 702. In 2014, that number was [92,707](#), and in 2015 it was [94,368](#). For every target under surveillance, there is at least one American whose communications are incidentally collected. But the total number could be in the millions. In a 2015 opinion, the [FISA Court](#) said Section 702 sweeps up "substantial quantities" of Americans' communications.

Scope of Surveillance: Foreign Intelligence Information

Section 702 allows the NSA to target *any* non-U.S. person for surveillance so long as a "significant purpose" of the surveillance is to collect "foreign intelligence information." There are two reasons why this results in surveillance that has nothing to do with national security.

The first problem is that "foreign intelligence information" has an extremely broad definition. While the first part of the definition includes information related to national security, the second part does not. The first part of the [definition](#) includes information that relates to our ability to protect against an attack by a foreign power; "sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power"; espionage by a foreign power, or our defense and security. The second part of the definition permits surveillance related to "the conduct of the foreign affairs of the United States." This allows surveillance concerning friendly diplomats and parties to trade negotiations, as well as political events, and even international business or other work.

- **Because of the broad definition of "foreign intelligence information", the NSA can use Section 702 to wiretap the phone calls, and monitor the emails and other electronic communications of Americans when they are in touch with anyone abroad like political or human rights activists, business partners, students, journalists, doctors, and lawyers.**

The second problem is that obtaining "foreign intelligence information" does not even have to be the primary purpose, let alone the only purpose, of conducting surveillance under Section 702.

- **This means that the NSA could shoehorn in surveillance under Section 702 where its primary purpose is unrelated to foreign intelligence information, such as a criminal investigation, per an FBI request. It just has to be able to claim that a significant purpose of the surveillance was also to collect "foreign intelligence information". Considering how broadly that is defined, it would not be difficult to imagine such a thing happening.**

For more information, contact Robyn Greene, Policy Counsel and Government Affairs Lead, New America's Open Technology Institute, at greene@opentechinstitute.org.

PRISM Surveillance

The PRISM surveillance program, often referred to as “downstream collection”, is used to obtain stored and real-time communications. It accounts for approximately [91 percent](#) of all collection under Section 702 surveillance programs.

Because the NSA must direct its surveillance abroad, it does not work directly with the internet providers to conduct the surveillance. Instead, the FBI serves as a liaison between the NSA and companies like Google, Facebook, Yahoo, Apple, and YouTube. The FBI serves the companies with directives that compel them to hand over all communications, on an ongoing basis, that are to or from selectors. Selectors are search terms that identify the targets, like email addresses or phone numbers.

- **Section 702 is intended to collect Americans’ communications with foreigners, so it results in the NSA incidentally obtaining [Americans’ content](#) from emails, video and voice chats, video conferences, VoIP, posted videos, photos, file transfers, account activities such as log-ins, details about social networking accounts, and “special requests”.**

Upstream Collection, “About” Communications, and Multi-Communication Transactions (MCTs)

Under Upstream Collection, the NSA collects communications content and metadata by wiretapping the undersea fiber optic cables, dubbed the “internet backbone”, which carry about [80 percent of global internet traffic](#). Like with PRISM, the NSA uses selectors to identify the information it seeks to collect, but in addition to communications “to” and “from” the target, the NSA also collects communications “about” the target. Whereas under PRISM, communications collected by the NSA are identified based on header (to/from) information, with Upstream Collection for “about” communications, the selector is in the content of the communication.

- **In order to identify relevant “about” communications, the content of every communication that transits the internet backbone is scanned.**
- **Because the vast majority of internet traffic transits these cables, the majority of Americans’ communications are scanned as part of Upstream Collection.**

There are two categories of internet communications: single communications transactions (SCTs) and multi-communication transactions (MCTs). SCTs are communications that go directly from one server to another, like when an internet user visits a webpage. MCTs are when a single internet transaction contains multiple discreet communications. When pressed for an example of an MCT, the [Office of the Director of National Intelligence explained](#) that an MCT could be when you open your email and what pops up on your screen is the header information and sample content for the top 15 or 25 emails in your inbox. Even though accessing your inbox is a single transaction, it results in the NSA capturing information about potentially dozens of communications if any one of those communications is “to”, “from”, or “about” the selector.

- **When engaging in Upstream Collection, the NSA collects discreet communications within MCTs that are not “to”, “from”, “or “about” the selector and that have nothing to do with the target or the purpose for surveillance. This includes wholly domestic communications, which are communications only between Americans with no foreign element.**
- **At one point, the FISA Court shut down Upstream Collection because of abuses with surveillance of MCTs that resulted in the NSA collecting [tens of thousands](#) of wholly domestic communications.**

For more information, contact Robyn Greene, Policy Counsel and Government Affairs Lead, New America’s Open Technology Institute, at greene@opentechinstitute.org.