CENTER FOR DEMOCRACY & TECHNOLOGY

Section 702: What It Is & How It Works

What Is It? Section 702 of the Foreign Intelligence Surveillance Act (FISA) is a statute that authorizes **the collection, use, and dissemination of electronic communications content** stored by U.S. internet service providers (such as Google, Facebook, and Microsoft) or traveling across the internet's "backbone" (with the compelled assistance of U.S. telecom providers such as AT&T and Verizon). Section 702 sunsets on **December 31, 2017**.

Are There Any Restrictions? Unlike "traditional" FISA surveillance, Section 702 does not require that the surveillance target be a suspected terrorist, spy, or other agent of a foreign power. Section 702 only requires that the targets be **non-U.S. persons located abroad**, and that a **"significant purpose"** of the surveillance be to obtain "foreign intelligence information" (the *primary* purpose of the surveillance can be something else entirely).

How Does Section 702 Work?

1) Certification: On an annual basis, the Attorney General and Director of National Intelligence make "certifications" authorizing 702 surveillance programs and submit these certifications to the Foreign Intelligence Surveillance Court (FISC) for approval. These certifications 1) identify **categories of foreign intelligence information** to be gathered, 2) contain **Targeting Procedures** and the **Minimization Procedures** approved by the AG that are meant to ensure 702 acquisition is limited to non-U.S. persons abroad, 3) attest that the targeting and minimization procedures and additional guidelines adopted to ensure compliance are consistent with the Fourth Amendment, 4) attest that a **"significant purpose"** of the program is to obtain foreign intelligence information, 5) attest that the program uses a U.S. electronic communications service provider, and 6) attest that the program complies with the limitations spelled out by the statute.

- If all the certification elements are present and the minimum requirements of the targeting and minimization procedures are met, the FISC *must* approve the 702 surveillance program. The FISC plays no role in making the actual targeting decisions (such decisions are made by the NSA, with "nominations" from the CIA and FBI).

2) Acquisition: *There are currently two known forms of 702 collection:*

- **PRISM** collection: the government collects all communications content **to or from** a targeted selector (such as an email address) directly from U.S.-based electronic communications service providers (such as Apple or Google). The NSA receives all raw (unminimized) PRISM-collected information and may also send such raw data to the CIA and FBI.
- **Upstream** collection: the government collects all internet transactions that contain communications **to, from, or "about"** a targeted selector as the transactions flow through network gateways controlled by U.S.-based providers. Only the NSA may receive raw Upstream-collected information, but it may send such information to the CIA and FBI once it has gone through the NSA's minimization process.

3) Querying and Use in Criminal Cases:

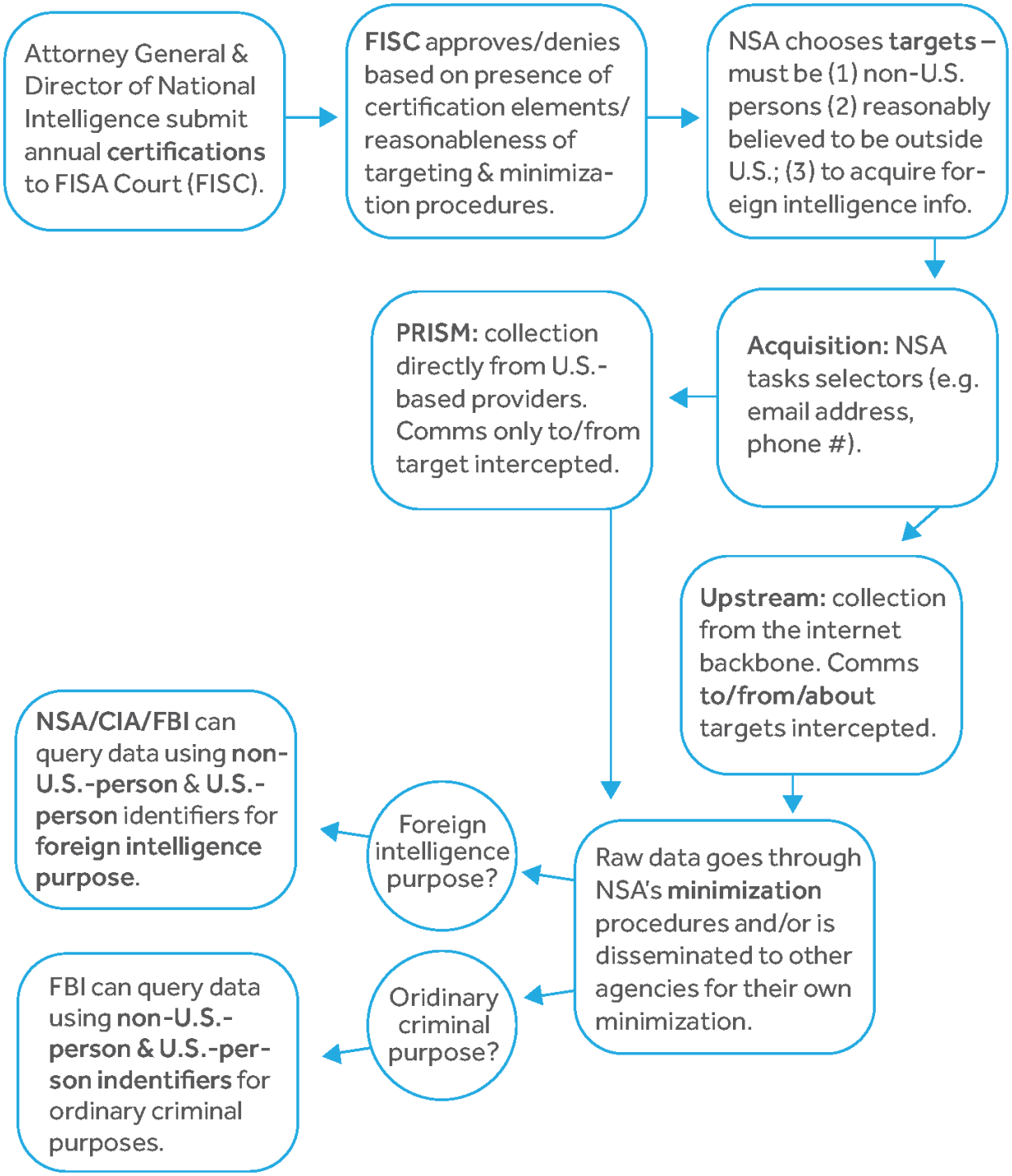
CENTER FOR DEMOCRACY & TECHNOLOGY

- **Querying 702 Information in Government Databases**: The NSA, CIA, and FBI are permitted to query 702-acquired information by using a variety of search terms. Each individual agency's own minimization procedures limit the search terms that analysts can use. However, it is unclear how these policies are enforced.
- **The Backdoor Search Loophole**: The NSA, CIA, and FBI are all permitted to search 702-acquired information with U.S. person identifiers (such as names or addresses). Critics have dubbed this the "backdoor search" loophole, because it enables the government to obtain information that would have otherwise required a warrant. Today, the NSA and CIA can only query 702-gathered information with a U.S. person identifier after creating a "statement of facts showing that a query is reasonably likely to return foreign intelligence information." However, **this restriction does not apply to the FBI**.
- **Use in Criminal Court**: 702-acquired information **may be used as evidence against U.S. persons in criminal court** for certain broad categories of "serious crimes." For investigations that do not fall into one of those categories, there is no restriction on using 702-acquired information to obtain other evidence that *can* be used in court. The use of information gathered under 702 without a warrant against U.S. persons creates an **end-run around the Fourth Amendment**, which requires a probable cause finding by an independent body.

See the reverse side for a flow chart of the 702 surveillance process. For more information, please contact Gregory T. Nojeim, Director of CDT's Freedom, Security & Technology Project, at gnojeim@cdt.org and view CDT's Statement for the Record about Section 702 reauthorization: https://cdt.org/?p=78385.

CENTER FOR DEMOCRACY & TECHNOLOGY

Section 702 Surveillance



1401 K Street NW, Suite 200, Washington, DC 20005