Forum for American Leadership

Section 702: What It Is, What It Isn't, and How It Works

March 17, 2023

Scores of intelligence successes over the last 15 years have depended on one section in one law that will expire at the end of this year. It has been renewed twice since its creation in 2008, each time with bipartisan support—between three-quarters and two-thirds of members voted in favor.

This year, 702 renewal may face new challenges that have little to do with the law itself. 702 authorities have become wrapped up in a debate about another part of the same, wide-ranging national security law, which featured prominently—and problematically—in FBI activity in 2016. Debates over those problems are important, but they should be kept separate from 702.

Allowing 702 to expire will blind us to threats when our adversaries are ramping up their espionage efforts. The IC would lose vital insight into Chinese spying activity, ransomware groups' plans, and terrorist plots. Intelligence officers and troops in the field would suddenly be blind to threats.

This brief from the Forum for American Leadership Intelligence Working Group examines some of the core questions about 702 collection, including what it does and does not allow, what safeguards are in place to protect Americans' privacy, and what happens if it expires.

What is 702?

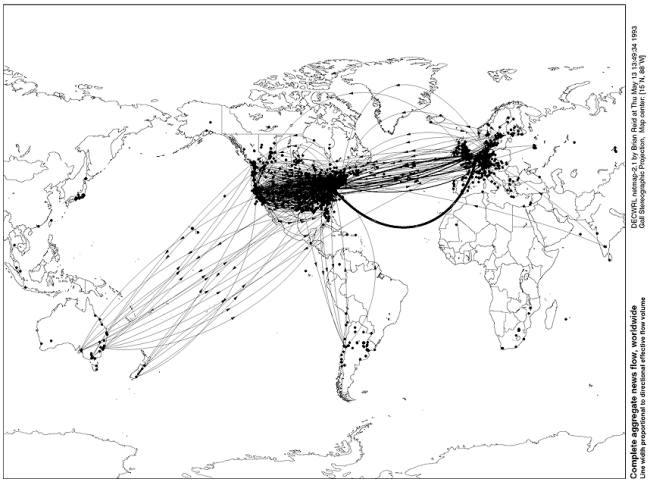
Section 702 of the *Foreign Intelligence Surveillance Act* allows NSA, CIA, FBI, and NCTC to collect intelligence about *non-U.S. persons* who are *overseas*.[1] It also places limits on that collection, specifically provisions to protect U.S. citizens and all people in the United States.[2] These agencies can compel U.S. electronics communications providers to provide information once a series of tests have been met. Those tests are the following:

1. The request must be for a non-U.S. person, and the non-U.S. person must be outside the U.S. at the time. If a target comes into the U.S., collection under 702 must cease.
2. The request must be about a specific phone number or email address, also called a "selector." A name is not enough. There is no "bulk," or indiscriminate, collection under 702.
3. The purpose of the collection has to be to acquire foreign intelligence. Agencies—even FBI—may not request information for a law enforcement or other purpose. Foreign intelligence is information that advances knowledge around a threat or foreign policy challenge, from counterterrorism, to defense against Russian cyber attacks, to Chinese counterintelligence.

[1] The term "U.S. person" encompasses a wide range of people. Under FISA, a U.S. person is a U.S. citizen, a legal permanent resident (green card holder), corporation incorporated in the United States, or unincorporated association substantially composed of U.S. citizens or legal permanent residents.

[2] For more information on 702, see Podcast Intelligence Matters with Michael Morell, Understanding Electronic Surveillance, guest Glen Gerstell, originally aired January 25, 2023.

Why do intelligence agencies need to involve U.S. companies in the request for non-U.S. persons' communications? It is easiest to answer this question with a map:



This is a map from 1993 of Usenet, an early internet bulletin board. From its earliest days, much of the Internet has run through the United States, and U.S. communications service providers have grown to serve the world. Exempting U.S. providers from providing information would block off access to most communications and give foreign actors a safe haven on U.S. services.

Why is 702 so important?
702 is the single most important source of statutory authority for NSA. A substantial portion of reporting comes from this one authority.

In the last 15 years, 702 collection has prevented at least two—and likely far more—terrorist attacks. 702 collection stopped both the plot to bomb the New York City subway system in 2009 and the attempt to attack the Portland, Oregon Christmas tree lighting in 2010. In 2014, 702 was critical in learning about ISIS attack planning and in finding and stopping ISIS leader Hajji Iman. In recent years, 702 collection has provided critical leads to catch Chinese spies, prevent IP theft, and stop ransomware attacks. 702 collection identified foreign ransomware attacks on critical infrastructure, allowing the government to respond to some attacks and prevent others. 702 revealed that a foreign adversary had used a cyber attack to steal sensitive military information, helped prevent weapons components from reaching hostile foreign actors, preempted attacks on U.S. troops, and protected CIA officers working in dangerous assignments overseas. General Paul Nakasone, director of the NSA, put it simply in a speech before the Privacy and Civil Liberties Oversight Board earlier this year: "We have saved lives because of 702."

If 702 is so valuable, what are the objections to reauthorizing?
Because 702 is part of the larger FISA law, some critics of other parts of FISA have also opposed 702. These criticisms usually cite privacy concerns—some with more specificity than others. For example, some have assumed 702 was used to surveil Carter Page in a 2016 counterintelligence investigation later found to be deeply problematic. But in the Page case, FBI used Title 1 FISA authorities, which require a warrant.

A more targeted criticism is the allegation that 702 makes it too easy to collect information on U.S. citizens and allows the FBI to access US person communications without a warrant, in situations where warrants would usually be necessary. FBI can access such communications in cases like investigating a crime with a foreign nexus or to notify potential victims.

Take this hypothetical example: NSA asks service providers to search for any emails sent by an address used by a Chinese intelligence officer in Beijing. They receive an email that officer sent to another Chinese intelligence officer in Taiwan. In the email, the two discuss an attempt to recruit an employee at a major U.S. defense firm we will call Stark Enterprises. The name of Stark's employee is "incidental" collection. FBI can then go to Stark Enterprises and provide a defensive briefing. After the brief, Stark searches their internal logs and discovers that the employee has accessed some of their most sensitive intellectual property on classified programs.

Because FBI has a dual counterintelligence and law enforcement mission, their interactions with 702 collection are complicated. FBI receives a small percentage of 702 collection—only 4.4 percent of targets—and only some of those are in contact with U.S. persons. That collection must be relevant to a pending full national security investigation. Then, FBI can only search for information about U.S. persons if the search is reasonably likely to return finished intelligence information or evidence of a crime. Said another way, FBI cannot run searches for Americans for a domestic crime where there's no indication of foreign involvement. If FBI would like to search for information on a person they are already investigating for a crime, they must notify the Foreign Intelligence Surveillance Court (FISC) and get a special order. While none of these steps are a search warrant, they are intensive procedures that have been approved by various courts.

Critics concerned about U.S. persons' privacy point to a very large number to support their concerns: in 2021, FBI queried 702 data more than 3 million times for information about a U.S. person. However, that comes with an even larger caveat: 1.9 million of those 3 million were to identify victims of a cyber attack and alert them that their systems were compromised. Protecting U.S. citizens in this way is part of FBI's mission; the victims are not suspects, so a search warrant is not a useful tool for notifying victims.

So what is stopping the government from abusing these powers?

In the 15 years 702 has been in effect, the three branches of government have put in place stringent oversight mechanisms with deliberate redundancy to "watch the watchers." Additional restrictions are in place surrounding U.S. persons to ensure protection of constitutional rights. Below is a list of the checks in place on 702 collection:

- The Attorney General and the Director of National Intelligence jointly certify that they authorize any targeting. An order to task a selector is good for only up to one year. Any renewal must be approved by the Attorney General and Director of National Intelligence.
- The government is expressly prohibited from targeting a non-U.S. person in order to learn about an American. For example, tasking collection on a non-U.S. person family member living abroad to gain insight into a U.S. person would be illegal.
- Any information incidentally collected about an American is handled consistent with court-approved procedures. Stringent "minimization" rules are also in place, by which names or identifying information about Americans are replaced with monikers like "U.S. person 1."

- All collection must be deleted within five years.
- Within NSA, the Inspector General, the Office of General Counsel, and a special 702 compliance division all oversee 702 collection. DoD has a designated unit to double check the decisions made by NSA.
- ODNI and DOJ check every targeting decision.
- The Privacy and Civil Liberties Oversight Board (PCLOB) began overseeing 702 operations in 2013, shortly after the Board was created, and issues regular reports on compliance with procedures.
- The Foreign Intelligence Surveillance Court reviews ODNI and AG certifications of procedures, conducts a comprehensive review of the program annually, and reviews allegations of noncompliance.
- Several Congressional committees have jurisdiction over 702 collection procedures, in particular the House and Senate Intelligence Committees, and review yearly transparency reports issued by ODNI.

What happens if 702 expires?

In January 2024, the Intelligence Community will be suddenly blind to communications about a range of threats to the U.S., from Chinese efforts to steal IP, to terrorist plots, to ransomware networks. Intelligence officers in the field won't be able to quickly verify if their asset is under surveillance or if they themselves have drawn the attention of a counterintelligence officer. U.S. and allied troops in harm's way will be blind to communications about their whereabouts and threats to their operations. At a time when China is aggressively escalating their intelligence operations—including sending balloons over military sites—we would be granting our adversaries an electronic safe haven.

A world without 702 will be dangerous in part because any alternative tool would be slower and, counterintuitively, less able to protect Americans' privacy rights. Other parts of FISA require a court order for each targeting decision. That would delay by days or weeks answers to often urgent questions, like "is my asset under surveillance? Should I meet with him?" The FISC would be quickly overwhelmed by urgent requests.

FISA 702 carries a small amount of risk to Americans' privacy in return for tremendous insight into a range of threats that affect life in the U.S. every day. That risk is mitigated comprehensively by oversight, training of personnel, and checks on use of the law. As General Nakasone said to the PCLOB in February 2023, "this authority plays an outsized role in protecting the nation, providing some of the U.S. government's most valuable intelligence on our most challenging targets. It provides unique information with minimal risk."

This paper is a product of the Forum for American Leadership's Intelligence Working Group.

The Forum for American Leadership (FAL) is a non-profit organization that presents expert analysis and national security recommendations to policymakers in Congress and the Executive Branch.