CENTER FOR DEMOCRACY & TECHNOLOGY

Updated November 2023

CDT Issue Brief: Properly Narrowing FISA Section 702 Targeting

FISA Section 702 permits overbroad designation of targets which endangers the privacy of Americans and foreigners and threatens U.S. business interests. This issue brief explains how this problem can be addressed while retaining access to necessary foreign intelligence information.

Problem: FISA Section 702 Permits Overbroad Targeting, Endangering Both Americans and Foreigners

FISA Section 702 authorizes warrantless surveillance. The goal of the law was to facilitate monitoring of foreign agents, terrorists, and intelligence operatives abroad, but its lax rules permit surveillance far beyond these types of legitimate targets. Any non-U.S. person located abroad can be designated as a target, so long as a significant purpose of doing so is to obtain foreign intelligence information. This is problematic because foreign intelligence information is defined extremely broadly, including a subclause — 50 USC 1801(e)(2) — that encompasses any information relating to the conduct of U.S. foreign affairs.

This unnecessarily broad definition opens the door to abuse through mass targeting of innocent people who are in no way suspected of wrongdoing or connected to malicious activities by foreign powers. For example, the current definition would allow, in certain circumstances, targeting the following types of individuals:

- A director screening an American produced film abroad
- An international businessperson
- Human rights activists and protesters
- Journalists covering public affairs
- Organizers of international sports events
- Humanitarian aid workers
- A scientist following fish migration paths
- Plant and wildlife conservation workers
- A musician on an international concert tour
- An expert examining the safety of consumer products

This type of unchecked surveillance causes an array of harms. Even though Americans cannot be FISA Section 702 targets, they will be swept up in this warrantless surveillance whenever they communicate with targets. The scale of FISA Section 702 surveillance has swelled massively: Since Congress last reauthorized the law, the number of publicly known targets has increased 118 percent, from 106,469 to 232,432.[1] Because FISA Section 702 is used to target so many individuals under such broad parameters, there is significant risk that Americans — even while speaking with friends, work colleagues, and relatives with no connection to security threats — will have their intimate conversations collected and subject to warrantless search by the government.

Permitting such broad targeting of innocent individuals also infringes on the privacy rights of foreigners abroad and threatens US business interests. The stability of U.S.-EU transatlantic data flows has been seriously compromised due to the breadth of FISA Section 702 surveillance. Over the past decade, the European Court of Justice has twice struck down U.S.-EU data flow agreements — first in *Schrems I* in 2015 and again in *Schrems II* in 2020 — due to inadequate safeguards on US surveillance. Last year the Administration took steps to lay the foundation for a new agreement, but absent significant reforms to FISA Section 702 by Congress, there is serious concern that agreements on data flows will simply be struck down again.[2]

Solution: Place reasonable guardrails on the purposes for which the government can designate FISA Section 702 targets

An effective remedy would be to establish a reasonably narrowed set of purposes for which the government can designate FISA Section 702 targets. There is already a model for a balanced targeting rule that protects the privacy of Americans and foreigners without compromising security needs can be put in place: Last fall the Administration issued an Executive Order on signals intelligence, which included a rule limiting the purposes for which signals intelligence (including via FISA Section 702) can be conducted. Based on this Executive Order, FISA Section 702 surveillance can only be conducted for one of the following purposes:[3]

1. Understanding the capabilities, intentions, and activities of foreign governments, militaries, factions, and political organizations in order to protect national security;
2. Understanding the capabilities, intentions, and activities of foreign organizations that pose a threat to national security;
3. Understanding transnational threats that affect security, such as climate change, public health risks, humanitarian threats, political instability, and geopolitical rivalries;
4. Protecting against foreign military capabilities and activities;
5. Protecting against terrorism and hostage-taking;
6. Protecting against espionage, sabotage, assassination, or other intelligence activities;
7. Protecting against development, possession, or proliferation of weapons of mass destruction;
8. Protecting against cybersecurity threats;
9. Protecting personnel of the United States and its allies;
10. Protecting against transnational criminal threats;
11. Protecting the integrity of elections and political processes, government property, and United States infrastructure; and
12. Advancing collection or operational capabilities in furtherance of the previous 11 objectives.

This year both the Privacy and Civil Liberties Oversight Board and the President's Intelligence Advisory Board issued reports on Section 702 that recommended codifying this list, a resounding endorsement of both its value and feasibility. This measure would ensure the continued application of this permissible purpose list without risk of the current executive order being supplanted or watered down, which the current Administration – and any future administration – could do unilaterally and in secret. Enshrining effective guardrails in statute would provide strong assurance to EU courts, protecting transatlantic data flows and aiding U.S. businesses. It would also allow US businesses to provide reassurances to their global users that they are not unfettered surveillance unrelated to security threats.

Alternatively, as CDT has previously suggested, Congress could require that whenever targets are designated for the purpose of collecting information related to foreign affairs (the problematic §1801(e)(2) subclause of the "foreign intelligence information" definition), there must be reasonable suspicion that those targets are agents of a foreign power. This would grant the government significant flexibility for designating targets based on national security needs — as well as reasonably restrained capacity to designate targets in order to gather information related to foreign affairs — while removing risk of mass surveillance of innocent individuals.

For more information, please contact Jake Laperruque, Deputy Director of CDT's Freedom, Security & Technology Project, at jlaperruque@cdt.org, or Project Director Greg Nojeim at gnojeim@cdt.org.

Endnotes

1 See, Jake Laperruque, "CDT Submitted Comments to PCLOB on FISA Section 702 Reform," The Center for Democracy & Technology, November 4, 2022. https://cdt.org/insights/cdt-submitted-comments-to-pclob-on-fisa-section-702-reform/ [https://perma.cc/EFN6-SHJ6].

2 See, Greg Nojeim and Iverna McGowan, "Report – Transatlantic Data Flows: More Needed to Protect Human Rights," The Center for Democracy & Technology, November 3, 2022. https://cdt.org/insights/report-transatlantic-data-flows-more-needed-to-protect-human-rights/ [https://perma.cc/Q9JW-3GE3].

3 The White House, "Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities," October 7, 2022. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/ [https://perma.cc/4V7Z-FJP7].