CENTER FOR DEMOCRACY & TECHNOLOGY

CDT Issue Brief: FISA Section 702 Key Reforms

This issue brief sets forth five key reforms related to Section 702 of the Foreign Intelligence Surveillance Act (FISA) that Congress should make to better protect civil rights and civil liberties and guard against abuse of its powerful authority to conduct warrantless surveillance.

Issue	Current Law	Needed Reform
Choice of Targets: Whom can the government target for surveillance?	The government can target anyone believed to be a non-U.S. person abroad for a broad set of reasons if the resulting acquisition obtains foreign intelligence information.	Limit the scope of permissible surveillance to specific and narrowly defined national security threats.
Backdoor Searches: In what circumstances can the government query FISA Section 702 data with a U.S. person's identifier?	The government can conduct U.S. person queries for law enforcement purposes without court approval 1) in the assessment stage of investigations, 2) for criminal investigations that relate to national security, 3) to mitigate a threat of serious bodily harm, or 4) whenever there is a dual law enforcement and foreign intelligence purpose.	Require court approval based on probable cause to conduct any U.S. person queries.
Use Limits: Can FISA Section 702 data be used for domestic law enforcement?	Yes. There are no limits on using FISA Section 702 data during domestic criminal investigations, and there is broad authority to use FISA Section 702 data in criminal court proceedings.	Limit use of FISA Section 702 data in domestic law enforcement to national security priorities.
"Abouts" Collection: Can FISA Section 702 be used to collect communications to which a target isn't even a party?	The government can resume its system of collecting communications "about" a target (even if not to or from the target) at any time with FISA Court approval and notice to Congress.	Limit collection under FISA Section 702 to communications to which the target is a party.
Notice: Are defendants notified when FISA Section 702 was used in their case?	Generally no; though the law requires notice when evidence derived from FISA Section 702 surveillance is used, a secret, likely narrow definition of "derived from," and parallel construction, both inhibit notice.	Require notice to defendants if FISA Section 702 data is used in a criminal investigation regarding their conduct.

I. Choice of Targets: Whom can the government target for surveillance?

FISA Section 702 permits warrantless surveillance of foreigners abroad. Such persons can be targeted to collect *foreign intelligence information*, a broad category that includes any information related to U.S. foreign affairs. This means any foreigner can become a FISA Section 702 target for engaging in innocuous activities such as journalism, activism, or international business. Such broad surveillance harms human rights, endangers the sustainability of U.S.-EU data flows, and increases the likelihood that Americans communicating with innocent individuals abroad are swept up in warrantless surveillance. Absent reasonable restraints, the number of publicly known FISA Section 702 targets has more than doubled since Congress last reauthorized the law. Congress should limit use of FISA Section 702 to collecting information related to a specific set of national security threats, such as those enumerated in the recently enacted Signals Intelligence Executive Order.[1]

II. Backdoor Searches: In what circumstances can government query §702 data with a U.S. person's identifier?

FISA Section 702 is based on the principle that surveillance cannot target U.S. persons or persons in the U.S., but this premise is undercut by the "backdoor search loophole." Using this loophole, FBI, CIA and NSA officials deliberately seek out Americans' communications in databases built on warrantless surveillance by querying the data with U.S. person identifiers. The FISA Court unearthed tens of thousands of U.S. person queries. This workaround undermines the key premise of FISA Section 702, as well as basic tenets of the Fourth Amendment.

Current law requires court approval for queries conducted for domestic law enforcement purposes (foreign intelligence queries are unrestricted), but the rule is riddled with loopholes. Warrantless queries can still occur: 1) during the

assessment stage of investigations; 2) in criminal investigations related to national security; 3) to mitigate threats to "life or serious bodily harm;" or 4) whenever a query has dual law enforcement and foreign intelligence purposes. Additionally, the complex nature of this system has caused mass compliance violations.[2] Protecting Americans from warrantless surveillance requires a clear rule: All queries for U.S. person information from Section 702 databases should require court approval based on probable cause.

III. Use Limits: Can FISA Section 702 data be used for domestic law enforcement?

Yes. FISA Section 702 authorizes warrantless surveillance — a power anathema to the Fourth Amendment — because it is directed at non-U.S. persons abroad for foreign intelligence purposes, as opposed to law enforcement. Yet, the law permits broad use of FISA Section 702 data for domestic policing – it can be used in anticipation of or in response to any crimes involving threats of serious bodily harm, cybersecurity, or criminal investigations that "relate to" national security. More importantly, limits on the use of Section 702 data apply when it is to be *introduced as evidence in court*; there are no restrictions on use of Section 702 data in investigations for any crime. The FISA Court has disclosed that the FBI queried Section 702 data for law enforcement investigations on health-care fraud, gang violence, corruption, and bribery, but these public revelations could just be the tip of the iceberg. Congress should build an effective barrier between warrantless FISA Section 702 surveillance and domestic policing. Specifically, it should limit use of information acquired or derived from FISA Section 702 surveillance to specifically enumerated national security-related offenses, and apply these limits to all stages of investigations.

IV. Abouts Collection: Can §702 be used to collect communications to which a target isn't even a party?

FISA Section 702 (like all forms of communications surveillance) was designed to monitor messages *to and from* surveillance targets. However, for many years, the government also used FISA Section 702 to collect data that merely *mentioned* targets (specifically selectors such as an email address or username) in the content of communications. This system — commonly referred to as "Abouts Collection" — defied the intended limits for FISA Section 702, and the basic concept of focusing surveillance on targets. Abouts Collection also suffered from technical problems that frequently led to overcollection. Because overcollection is illegal, the FISA Court required discontinuation of Abouts Collection in 2017, subject to these issues being fixed. FISA Section 702 currently does not prohibit About Collections from resuming; it merely requires notice to Congress if it resumes. Surveillance should focus exclusively on targets – Congress should clearly prohibit Abouts Collection.

V. Notice: Are defendants notified when FISA Section 702 was used in investigating their case?

Given the potentially broad use of FISA Section 702 surveillance in domestic law enforcement, it is important that defendants receive notice when FISA Section 702 was used to investigate them. Notice affords them the opportunity to challenge such surveillance if it was not conducted lawfully. However, notice is frequently blocked for two reasons: First, the Justice Department employs a secret interpretation of what it means for evidence to be "derived" from FISA (which triggers notice requirements), giving the government the ability to take an unnaturally narrow view of when notice is necessary. Second, agencies often employ "parallel construction" — a technique where information discovered from one source, such as FISA Section 702, is artificially rediscovered via another method — to hide the surveillance tool originally used. The law should clearly require notice whenever evidence would not have been available but for use of FISA.

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

Endnotes

1 The Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities (signed October 7, 2022) requires signal intelligence be conducted only for the following purposes: 1) Gathering intelligence on foreign governments and militaries; 2) Gathering intelligence on foreign organizations that pose a threat to national security; 3) Understanding transnational threats that affect security; 4) Protecting against foreign military activities; 5) Protecting against terrorism and hostage-taking; 6) Protecting against espionage, sabotage, assassination, or other intelligence activities; 7) Protecting against 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.

2 The FISA Court issued two separate opinions in 2019 and 2020, each documenting how even the lax rules that currently exist have been violated on a mass scale. The FBI has conducted "batch queries," that are effectively bulk queries of thousands of U.S. persons in one fell swoop. Some queries have focused on purely domestic law enforcement issues, such as health-care fraud. The FBI has also conducted queries on a significant number of U.S. persons totally unrelated to any criminal investigations, monitoring "business, religious, civic, and community leaders" applying to the FBI's Citizen Academy program, individuals conducting maintenance services at field offices, and crime victims. None of these queries were predicated on probable cause or received any court authorization.