Statement for the Record
for Senate Judiciary Committee Hearing,
"Oversight of Section 702 of the Foreign Intelligence Surveillance Act and Related Surveillance Authorities"
Submitted by Jake Laperruque,
Deputy Director of the Security and Surveillance Project of the
Center for Democracy & Technology

June 12, 2023

The Center for Democracy & Technology ("CDT") submits the following statement for the record regarding Section 702 of the Foreign Intelligence Surveillance Act ("FISA"). CDT is a 501(c)3 nonpartisan nonprofit organization that works to promote democratic values by shaping technology policy and architecture, with a focus on equity and justice. Among our priorities is preserving the balance between security and freedom. We have long expressed concerns that FISA Section 702 permits overbroad surveillance and lacks adequate safeguards, threatening the privacy and civil liberties of both individuals abroad and within the United States.

Any reauthorization of FISA Section 702 must be accompanied by significant reform and establishment of new safeguards to end misuse of this authority, which has occurred with shocking frequency in recent years. This statement will focus on two key reforms: 1) closing the "backdoor search loophole" by requiring a warrant for US person queries of communications collected under Section 702, and 2) narrowing Section 702 surveillance to genuine security threats. In addition to these issues, a broad range of other reforms are critical to a successful FISA Section 702 reauthorization. [1]

I. Congress should close the "backdoor search loophole" by requiring a warrant for US person queries

FISA Section 702 significantly impacts Americans because it is regularly used to seek out and review Americans' communications that were collected without a warrant. Although FISA Section 702 is often framed by its proponents as a foreign-focused surveillance system that only targets foreigners located abroad, it is inevitable and expected that many Americans' private communications will be swept in. This occurs via "incidental collection" — whenever Americans speak with a foreign target, their communications are subject to warrantless surveillance. And because the scale of permissible targets is incredibly broad (targets need not have any suspected ties to foreign powers, security threats, or malicious activities), Americans speaking with innocent foreigners abroad such as friends, family, and business associates have their communications collected.

The government can — and frequently does — query databases of FISA Section 702-acquired communications to deliberately seek out these Americans' conversations without any judicial oversight or even suspicion. The intelligence community maintains that US person queries do not constitute a search because they are made on data already in the government's possession. This distinction does not justify the harm to privacy: these queries have *the same effect as a direct search* — government officials deliberately seek out, review, and use US persons' private communications without ever going through the checks and rules required for upfront searches. Individuals face the same harm to their privacy rights, but without any of the protections.

The scale and nature of US person queries reflect how FISA Section 702 has morphed into a domestic surveillance system. Last year the FBI conducted over 204,000 US person queries, an average of over 558 per

[1] These reforms include expanding the role of FISA Court amici and instituting other court reforms, expanding access to courts to litigate overbroad surveillance, providing defendants with notice when Section 702 was used in investigations, and ensuring that if Section 702 is reformed, improper surveillance practices are not simply shifted to other methods such as purchases of data from brokers or monitoring via Executive Order 12333. We focus here on U.S. person queries and scope of surveillance because they are priority reforms likely to be discussed at this hearing, and because we plan to address the additional reforms in subsequent comments to the Committee.

day.[2] While FISA Section 702 was created to respond to international security threats, today US person queries are used for an array of domestic law enforcement activities totally disconnected from national security such as health care fraud, bribery, and public corruption.[3] Even more troublingly, FISA Section 702 also is used to seek out the private communications of Americans in no way suspected of wrongdoing. The government has mis-used FISA Section 702 data by querying with the identifiers of US persons such as:[4]

- Over 100 Black Lives Matter protesters
- A group of 19,000 donors to a Congressional campaign
- A sitting US Congressperson
- Relatives of an FBI official performing a query
- Journalists
- A "local political party"
- Political commentators
- Current and former US government officials
- Victims who reported crimes to the FBI
- Law enforcement sources
- Individuals applying to work in local law enforcement
- Workers conducting maintenance at FBI offices
- Business, religious, and community leaders who applied to participate in the FBI's "Citizens Academy" program
- College students participating in a "Collegiate Academy" program

These queries are non-compliant because they do not meet the requirements for conducting them that the Attorney General imposed in guidelines that Congress required. For many of these queries, "the [intelligence analyst] struggled to articulate a 'reasonable belief' that the queries would return foreign intelligence information or evidence of a crime," as required by Attorney General guidelines, or compliance assessments determined there was no reasonable basis to believe the queries would return such information.[5]

In 2018, when Congress last reauthorized Section 702, it established a warrant requirement for US person queries in some limited situations. But this system is riddled with exceptions that subsume the rule, and in its complexity has fostered a culture of noncompliance. The warrant requirement only applies to queries made "in connection with a predicated criminal investigation," permitting the FBI to make such queries in "assessments" when it doesn't even have the minimal level of suspicion required for opening a preliminary investigation. This means that situations where the government has the *least* suspicion of wrongdoing are those in which it has the *most* power to conduct US person queries without court authorization. Further, the warrant requirement does not apply to any queries that "relate to national security" or might mitigate "a threat to life or serious bodily harm."

---

[2] Office of the Director of National Intelligence, *Statistical Transparency Report Regarding use of National Security Authorities Annual Statistics for Calendar Year 2022*, April 2023. https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf. In addition to the 204,090 query number, this report also includes a "de-duplicated query figure" of 119,383, the number of unique identifiers used in the queries. This lower number poorly reflects FBI practices, as it excludes any instances of the same US person being subject to multiple queries, which could be made on different dates, by different personnel, for different reasons, and return entirely different communications.

[3] Memorandum Opinion and Order (FISA Ct. Nov. 18, 2020) available at https://perma.cc/8U2N-5GYP (hereinafter *FISA Court 2020 Opinion*).

[4] For information on the full set of examples listed below, see, Memorandum Opinion and Order (FISA Ct. Apr. 21, 2022), available at https://perma.cc/26EN-YUHS (hereinafter, *FISA Court 2022 Opinion*); Office of the Director of National Intelligence, 22nd Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (August 2021), https://perma.cc/JB3J-NXWP (hereinafter, *22nd FISA Section 702 Compliance Report*); Office of the Director of National Intelligence, 24th Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (December 2021), https://perma.cc/E76T-RKBG (hereinafter, *24th FISA Section 702 Compliance Report)*; *FISA Court 2020 Opinion*; Memorandum Opinion and Order (FISA Ct. Dec. 6, 2019) (hereinafter, *FISA Court 2019 Opinion*, available at https://perma.cc/94E9-A6BE.

[5] *FISA Court 2022 Opinion*; *22nd FISA Section 702 Compliance Report*; *24th FISA Section 702 Compliance Report*.

These categories are overbroad and undefined in statute, giving the government immense flexibility to claim queries have some nexus to either category.

The convoluted nature of these rules has also bred a culture of noncompliance, with the FISA Court stating that the FBI has "conducted a large number of suspicionless queries," engaged in "widespread violations of the querying standard," and displayed "a misunderstanding of the querying standard — or indifference to it."[6] Despite claims that new internal rules and measures have solved these issues, noncompliance still occurs at a shocking rate. Even with the FBI's newest internal reforms, an internal audit found a four percent noncompliance rate.[7] Given that the FBI conducted over 204,000 US person queries in 2022, this means the Bureau conducted over 8,100 US person queries last year in violation of rules, an average of 20 noncompliant queries for US persons' communications *every day* (and that assumes the FBI's internal assessment is accurate and does not understate noncompliance). The only way to stop this pattern of improper conduct and protect Americans' privacy is to put a judge between the FBI and the data it seeks by imposing a clear and consistent warrant rule for US person queries.

Congress should also reject the FBI's assertion that Congress should permit warrantless "defensive searches" that focus on a target of foreign influence operations or victims of cyberattacks. The FBI argues that when its queries are for the data of these categories as opposed to investigative targets, they should be excluded from any warrant requirement. Such an exception would continue to permit, for example, querying to find the communications of Congressman Darin LaHood, as was recently disclosed not by the FBI, but by Rep. LaHood himself.[8] The queries relating to 19,000 donors to an undisclosed congressional campaign are an astounding example of the "defensive searches" such an exception would open the door to.

Additionally, history is filled with chilling examples of how easily the notion of conducting defensive surveillance to protect Americans from foreign influence can be a pretense for politically motivated surveillance abuse. For example, J. Edgar Hoover authorized the monitoring of Dr. Martin Luther King Jr. ostensibly to defend against alleged communist influence efforts aimed at King and other civil rights leaders.[9] In reality, it was motivated by Hoover's racism and hatred of the civil rights movement.[10]

Detecting and defending against purported foreign influence and subversion was a frequent excuse for monitoring political dissidents—such as the antiwar movement, Black activists, students, and other left-leaning groups—throughout the 1960s and 70s for the abusive COINTELPRO surveillance program. The FBI even described defensive surveillance as something that "offers us a fertile field to develop valuable intelligence" on leftist political groups despite a lack of evidence of actual foreign danger.[11] Justifying spying on vulnerable communities and dissidents as a defensive measure to protect against foreign actors has continued into the 21st century. After the September 11 attacks, the New York Police Department, with federal support, engaged in mass surveillance of Muslim communities. They justified monitoring mosques, community centers, student groups, and the daily lives of average Americans—actions with serious harms—as necessary to guard against influence and infiltration by foreign actors like al Qaeda.[12]

---

[6] *FISA Court 2020 Opinion*; see also, Memorandum Opinion and Order (FISA Ct. Oct. 18, 2018) available at https://perma.cc/9CSR-63QM; see also, Memorandum Opinion and Order (FISA Ct. Dec. 6, 2019) available at https://perma.cc/FTJ7-LDLG.
[7] Federal Bureau of Investigations Office of Internal Auditing, "FISA Query Audit," May 10, 2023. https://int.nyt.com/data/documenttools/fisa-query-audit-5-10/d9d8e20bafef27c8/full.pdf.
[8] Charlie Savage, New York Times, "F.B.I. Feared Lawmaker Was Target of Foreign Intelligence Operation," April 13, 2023. https://www.nytimes.com/2023/04/13/us/politics/fbi-darin-lahood.html.
[9] The Martin Luther King, Jr. Research & Education Institute, Stanford, "Federal Bureau of Investigations (FBI)." https://kinginstitute.stanford.edu/encyclopedia/federal-bureau-investigation-fbi.
[10] Alvaro Bedoya, Slate, "The Color of Surveillance," January 18, 2016. https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-luther-king-says-about-modern-spying.html.
[11] Church Committee Report, Book II, April 26, 1976. https://perma.cc/8WWY-TETS.
[12] Saher Khan and Vignesh Ramachandran, *PBS News Hour*, "Post-9/11 surveillance has left a generation of Muslim Americans in a shadow of distrust and fear," September 16, 2021. https://www.pbs.org/newshour/nation/post-9-11- surveillance-has-left-a-generation-of-muslim-americans-in-a-shadow-of-distrust-and-fear.

The decades-long pattern shows that a blank check for warrantless "defensive" searches of Americans' communications collected pursuant to Section 702 could be abused for political or other purposes. To be sure, there are certain to be many genuine situations where the FBI and other intelligence agencies want to investigate and root out foreign influence efforts or other nefarious actions by foreign actors targeting Americans. The government should be able to pursue those investigations through its broad arsenal of lawful investigative powers, including appropriately predicated and judicially authorized searches of communications. This can also include US person queries related to victims and targets of foreign malfeasance, and Title III Wiretap warrants permit surveillance based on a probable cause showing that the government's actions will return evidence of wrongdoing.[13] Therefore, there could still be victim-focused queries in this realm—such as for information relating to a cyberattack—so long as they are still properly predicated on probable cause and subject to independent approval by courts. These key checks are necessary to prevent the abuses that have marred "defensive" surveillance for decades.

There's a reason the Fourth Amendment does not prohibit only "unreasonable *offensive* search and seizures": no matter what the government's motive is or is purported to be, we need a strong and consistent shield to protect our citizens and our democracy. Before searching for an American's private communications, get a warrant.

II. *Congress should narrow the parameters of Section 702 targeting to genuine security needs*

In addition to closing the backdoor search loophole, Congress should narrow the scope of FISA Section 702 surveillance. FISA Section 702 permits the overbroad designation of targets, which endangers the privacy of Americans and foreigners, and threatens US business interests. Congress enacted this law 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-US 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 in a subclause — 50 USC 1801(e)(2) — that encompasses any information relating to the conduct of US 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:[14]

- 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. For example, even though Americans cannot be FISA Section 702 targets, they will be swept up in this warrantless surveillance whenever they communicate with targets. And 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.[15] 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,

[13] 18 USC 2518(3).
[14] For additional information on these and other types of potential overbroad Section 702 targets, see, Mana Azarmi, The Center For Democracy & Technology, "Urgent Fix Needed: USA Liberty Act Needs To Better Focus Surveillance Under FISA 702," October 20, 2017. https://cdt.org/insights/urgent-fix-needed-usa-liberty-act-needs-to-better-focus-surveillance-under-fisa-702/.
[15] See, Jake Laperruque, "CDT Submitted Comments to PCLOB on FISA Section 702 Reform," The Center for Democracy &; Technology, November 4, 2022. https://perma.cc/EFN6-SHJ6

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 US-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 US-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 future agreements on data flows will simply be struck down again.[16] The ramifications of inaction to U.S. businesses will be severe: Just last month an American company – Meta -- received a $1.3 billion fine due to concerns that the data of Europeans that it transfers was vulnerable to overbroad U.S. surveillance.[17]

Congress can ensure FISA Section 702 targeting is properly limited in two distinct ways. First, it 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.

Alternatively, another effective remedy would be to establish a reasonably narrowed set of purposes for which the government can designate FISA Section 702 targets. There is strong basis to believe that 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 a set of thirteen enumerated purposes, which, collectively, are narrower than the statutory purposes for which Section 702 surveillance can be conducted. If the executive believes it can meet operational needs while voluntarily adhering to these limits, it should have no objection to them being codified into statute. Doing so would ensure their continued use without risk of the current executive order being supplanted or watered down, which the current Administration – and any future administration – could do unliterally and in secret. Enshrining effective guardrails in statute would provide strong assurance to EU courts, protecting transatlantic data flows and aiding US businesses.

***

We thank the Senate Judiciary Committee for considering this statement and our recommendations, and we look forward to working with members of the Committee as they examine how best to protect privacy, civil rights, and civil liberties as it considers possible reauthorization of FISA Section 702. For further information, please contact Jake Laperruque, Deputy Director of the Security and Surveillance Project at the Center for Democracy & Technology, at jlaperruque@cdt.org.

[16] 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://perma.cc/Q9JW-3GE3.
[17] Adam Satariano, *New York Times*, "Meta Fined $1.3 Billion for Violating E.U. Data Privacy Rules," May 22, 2023 https://www.nytimes.com/2023/05/22/business/meta-facebook-eu-privacy-fine.html.