The University of Texas at Austin
Strauss CENTER
for International Security and Law

REVIEW AND REFORM: THE FOREIGN INTELLIGENCE SURVEILLANCE ACT AND EXECUTIVE ACCOUNTABILITY

Prepared Statement of Adam I. Klein

Director, Robert Strauss Center for International Security and Law
University of Texas at Austin

Before the U.S. Senate Committee on the Judiciary

January 28, 2026

Chairman Grassley, Ranking Member Durbin, and Members of the Committee, thank you for inviting me to testify today.

Introduction

In the digital era, much of the most valuable foreign intelligence can be found on networks in the United States. Section 702 of the Foreign Intelligence Surveillance Act allows our government to gather that information safely, at very low cost, at a speed and scale that would otherwise be impossible. The government uses information from 702 to protect our people and our troops abroad from terrorists, foreign spies, narco-traffickers, hostile military action, and other threats. Allowing 702 to sunset would be an unparalleled strategic blunder.

Section 702 has been in force for nearly two decades. During that time, there has not been one documented case of intentional abuse of the program. Americans are not and cannot be targets under 702: it can only be used to target foreign nationals, located overseas, who are likely to possess foreign intelligence information.

There have been *unintentional* compliance incidents, including noncompliant queries of Section 702 data. But just two years ago, in the Reforming Intelligence and Securing America Act (RISAA), Congress enacted dozens of reforms to sharpen compliance with FISA rules. Those reforms are working: The Department of Justice's Office of the Inspector General recently reported that "the FBI has implemented all of RISAA's querying reforms" and found that "the

number of noncompliant queries identified in NSD oversight reports has been reduced substantially post-RISAA."[1]

Congress can use this sunset to fine-turn certain of RISAA's reforms—most notably, streamlining RISAA's requirement of congressional access to FISC proceedings.

Congress should not, however, require a court order for the FBI to use query terms pertaining to U.S.-persons to call up records from its database of information already collected under 702. These queries' impact on privacy is modest: Section 702 collects information only by targeting foreign intelligence targets overseas, and the FBI's 702 database receives only a small fraction of that overall collection. And these queries are valuable: the government has used them to prevent terrorist attacks in the United States, interrupt proliferation schemes, and respond to damaging cyberattacks on our critical infrastructure. Requiring a court order would effectively prevent such queries early in an investigation, when they are most useful.

I. Section 702 Has Proven Indispensable and Should be Made Permanent

America's central position in global digital networks yields profound benefits for our national security. Because people around the world use American digital infrastructure, a vast amount of foreign data touches the United States. That includes the communications of many priority intelligence targets: foreign spies, terrorists, cartel members, weapons smugglers, and the like. This makes it possible to collect valuable intelligence on them from inside the United States, even when they are physically located abroad.

Section 702 is the legal key that enables the U.S. government to do this at scale. Under the Foreign Intelligence Surveillance Act, electronic surveillance or physical search inside the United States traditionally required an individualized court order. Getting such an order is a laborious process culminating in individualized review by a FISA Court judge. That level of scrutiny makes sense for a U.S. citizen secretly accused of being an agent of a foreign state or terrorist group. But it does not make sense for a non-citizen overseas who has no connection to the United States and no rights under the Fourth Amendment.[2]

Congress resolved this in the FISA Amendments Act of 2008, which created 702, by enabling the intelligence community to target *non-U.S. persons*, *located outside the United States*, without an individualized court order. Instead, the FISA Court annually approves the

[1] *A Review of the Federal Bureau of Investigation's Querying Practices Under Section 702 of the Foreign Intelligence Surveillance Act*, at iii (Oct. 2025).

[2] *See United States v. Verdugo-Urquidez*, 494 U.S. 259, 266 (1990) ("The available historical data show, therefore, that the purpose of the Fourth Amendment was to protect the people of the United States against arbitrary action by their own Government; it was never suggested that the provision was intended to restrain the actions of the Federal Government against aliens outside of the United States territory.").

rules under which the government conducts 702 collection. The government has now used 702 lawfully for nearly 20 years, with incalculable benefit for American and global security.

The jargon-term "702" creates the misimpression that this law authorizes a mysterious, unusual form of intelligence collection. It does not. At bottom, 702 is simply about collecting foreign intelligence from the internet, and doing so from here in the United States rather than at collection points overseas that are less capable and secure.

As the internet and the digital economy subsume ever more of the world's business, government, and personal communications, all serious intelligence powers, if they have not done so already, will come to rely on collecting foreign intelligence from the internet in this way. To illustrate: a paper published by my organization, the Strauss Center for International Security and Law at the University of Texas at Austin, noted that as of 2020, Germany's intelligence service, the BND, was collecting trillions of internet transactions *per day* from the DE-CIX internet connection hub in Frankfurt.[3]

Our geopolitical adversaries, meanwhile, harvest online data with none of 702's statutory restrictions, court review, or oversight. Russia's SORM system, for example, gives security and intelligence services "direct access to telecommunications traffic," "landline and mobile communications[,] … internet traffic, Wi-Fi, and social media," all preserved in a "searchable database."[4]

It is not plausible that the United States would be the only major nation that does not collect foreign intelligence at scale from internet infrastructure within its own borders. Nor would it be right to blind ourselves in this way, while thousands of servicemembers, intelligence officers, and diplomats, whom this intelligence could help protect, are bravely serving the American people in hazardous posts around the world.

Section 702's value for national security has been amply documented, but it bears repeating: Section 702 is likely our government's single most valuable intelligence-collection authority. According to the intelligence community, in 2023, a remarkable 60% of the articles in the President's Daily Brief contained information reported by NSA from Section 702 collection.[5] Section 702 has helped authorities track down leaders of al Qaeda and ISIS, prevent active

---

[3] Thorsten Wetzling, *National Security Surveillance in Germany*, Robert Strauss Center for International Security and Law *Safe and Free* Series Paper, at 10 (Nov. 2023) ("More generally, it was reported in 2020 that the BND copies 1.2 trillion IP connections per day at DE-Cix alone."), https://safeandfree.io/wp-content/uploads/2023/11/Germany_Surveillance_FINAL.pdf.

[4] Recorded Future, *Tracking Deployment of Russian Surveillance Technologies in Central Asia and Latin America* (Jan. 7, 2025), https://www.recordedfuture.com/research/tracking-deployment-russian-surveillance-technologies-central-asia-latin-america.

[5] *FISA Section 702 Value*, Feb. 14, 2024, https://www.intelligence.gov/assets/documents/702-documents/FISA_Section_702_Vignettes-20240214_Final.pdf.

terrorist plots in the United States,[6] disrupt fentanyl trafficking, protect U.S. troops abroad, and prevent or mitigate numerous damaging cyberattacks against the U.S. homeland.

Recent statutory changes and events overseas have likely made Section 702 collection even more relevant. In RISAA, Congress added international counternarcotics to FISA's definition of foreign intelligence information.[7] The government then sought, and the FISA Court approved, a new "Certification D" permitting the government to employ 702 to "acquire 'foreign intelligence information' concerning the international production, distribution, and financing of illicit opioids, [redacted] cocaine," and the chemical precursors for those drugs.[8] Combating international narcotrafficking and the designated Foreign Terrorist Organizations[9] involved in it has since become a top-tier defense and intelligence priority. We can reasonably assume that 702 is daily producing actionable intelligence on the cartels and any foreign states that assist them.

For these reasons, Section 702 should be made a permanent feature of American intelligence law. Losing collection from 702 would do relatively little to protect Americans' civil liberties—the targets are foreign, after all—but would dramatically increase the risk of intelligence failures on the order of Pearl Harbor or 9/11. However, if Congress cannot enact a permanent reauthorization, the eight-year extension proposed by this Committee would be a significant improvement on the current two-year cycle.

II. RISAA Markedly Improved Safeguards Around FISA Collection

There has never been a documented case of using 702 to intentionally target an American. That is an uncrossable red line, and must remain so. RISAA clarified once again that 702 "has always prohibited, and continues to prohibit, the intelligence community from targeting a United States person for collection of foreign intelligence information," and added a new requirement that the Department of Justice review each target to ensure that 702 is not being misused for that purpose.[10] Because of the many safeguards that exist, even unintentional noncompliance with this provision is extremely rare.[11]

---

[6] *See* NSA, *FISA Section 702: Foreign Intelligence Mission Outcomes*, https://www.nsa.gov/Portals/75/702%20Foreign%20Intelligence%20Outcomes.pdf (discussing Zazi case).

[7] Pub. L. No. 118-49 (Apr. 20, 2024) (RISAA), § 23.

[8] *See* No. 702(j)-24-04 (F.I.S.C. Apr. 9, 2025).

[9] *See* U.S. Department of State, *Foreign Terrorist Organization Designations of Tren de Aragua, Mara Salvatrucha, Cartel de Sinaloa, Cartel de Jalisco Nueva Generacion, Carteles Unidos, Cartel del Noreste, Cartel del Golfo, and La Nueva Familia Michoacana*, 90 Fed. Reg. 10,030 (Feb. 20, 2025).

[10] RISAA § 4.

[11] *See* U.S. Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (Sept. 28, 2023), Annex B (Statement of Members Beth Williams and Richard DiZinno), at B-12 (noting compliance rates consistently above 99%, and usually above 99.9%).

Just two years ago, Congress added dozens of new safeguards to the FISA process. Some reforms, which are described in more detail below, related to U.S.-person queries of 702 collection. Others were designed to make the FISA process more searching. These include:

- Requiring appointment of an amicus curiae in every annual review of 702 certifications
- Requiring designation of a lawyer to scrutinize every application to monitor a U.S. person
- Mandating that all factual assertions be made in a sworn statement
- Requiring extensions to go to before the same judge who approved the initial surveillance
- Barring undisclosed political opposition research from FISA applications
- Restricting the use of press reports in FISA applications, and
- Increasing penalties for misconduct by people involved in preparing FISA applications

Many of these changes were designed to prevent political misuse of the FISA process—a necessity after the inappropriate surveillance of former Trump campaign official Carter Page. That surveillance took place under Titles I and III of FISA, not 702, which cannot be used against Americans. Nonetheless, the Page case highlighted the importance of firmly separating intelligence from politics and the need to restore trust in the institutions that superintend both "traditional" FISA (Titles I and III) and Section 702. RISAA's many important changes should be given time to take effect before Congress makes other deep changes to the statutory scheme.

III. This Reauthorization is an Opportunity to Strengthen RISAA's Provision on Congressional Access to FISC Proceedings

RISAA sought to give Members of Congress and appropriately cleared, designated staff greater access to proceedings of the Foreign Intelligence Surveillance Court.[12]

As this hearing reminds us, under our Constitution, Congress constitutes and funds lower federal courts, including the FISA Court.[13] To perform that constitutional role effectively, Congress must be able to form a detailed impression of the Court's process. RISAA aimed to empower Congress to do that by authorizing the bipartisan leaders of both houses, the intelligence committees, and the judiciary committees to attend FISC and FISC-R proceedings, and to designate two appropriately cleared staff members to attend on their behalf. It also

[12] Pub. L. No. 118-49 (Apr. 20, 2024), §§ 5(d) (attendance at FISC and FISC-R proceedings), 8 (transcripts).

[13] U.S. Const. art. I §§ 8 ("The Congress shall have Power … To constitute Tribunals inferior to the supreme Court"), 9 ("No Money shall be drawn from the Treasury, but in Consequence of Appropriations made by Law").

required transcripts of FISC proceedings, which would then be available upon request by the relevant congressional committees.

Unfortunately, complicated procedures introduced by the Executive Branch (which does not, of course, have inherent authority to control access to courts) appear to have made it difficult for Congress to effectively exercise this new prerogative. Section 2 of the proposed "FISA Accountability and Extension Act of 2026" would remove those obstacles while leaving the door open for truly essential security restrictions. To the extent that this provision raises concerns about third-party information subject to the originator-control principle, those should be resolved by consensual discussions between Congress and the Executive Branch.

IV. Requiring a Judicial Order For 702 Database Checks is Unnecessary and Unwise

Many of RISAA's reforms were directed at "U.S.-person queries": electronic searches within government databases of information already collected under Section 702 in order to find information about known or suspected U.S. persons. Most notably, RISAA:

- Limits the FBI personnel who can authorize U.S.-person queries
- Bars political appointees from being involved in U.S.-person queries
- Requires the Department of Justice to audit all U.S.-person queries within 180 days
- Requires annual training on the FBI's querying procedures
- Requires the FBI Deputy Director to approve the most politically-sensitive queries
- Requires attorney review and approval of other sensitive U.S.-person queries
- Requires a prior written justification for all U.S.-person queries
- Mandates that data systems require users to opt into querying 702 data
- Requires the FBI to notify congressional leadership of queries pertaining to Members of Congress, and
- Bars U.S.-person queries unrelated to national security

Even before RISAA, the number of U.S.-person queries conducted by the FBI had already declined by orders of magnitude as a result of greater scrutiny and constraints imposed by the

Attorney General and the FISA court: from nearly 4 million in 2021[14] to only 5,518 in 2024.[15] For many of those remaining queries, the U.S. persons are *victims* of hacking or espionage threats; the queries enable the FBI and other agencies to warn and protect those Americans.[16] Compliance has also improved "substantially" since RISAA, as recently confirmed by the Justice Department's Office of Inspector General.[17]

a. *Database checks can prevent terrorist attacks in the United States*

Past tragedies, from 9/11 to Fort Hood, have left an indelible lesson for American counterterrorism: to stop terrorist attacks, agencies must, at a minimum, connect the dots between pieces of information the government already has.

For example, the government had collected emails from the future Fort Hood shooter, U.S. Army Major Nidal Hasan, and terrorist cleric Anwar al Awlaki. One of the emails said: "I would assume that a suicide bomber whose aim is to kill enemy soldiers or their helpers, but also kills innocents in the process is acceptable."[18]

The Webster Commission, which investigated the attack, found that investigators looking at Hasan "erred in failing to search the database in which electronic communications were stored, if only to determine whether al-Awlaki had replied to Hasan's messages."[19] For that reason, the Commission devoted several recommendations to new, integrated search tools to help the FBI to "master the ever-expanding amount of electronic data in its possession."[20]

Similarly, the 9/11 Commission found that information from intelligence agencies "often failed to make its way to criminal investigators" at the Federal Bureau of Investigation—a phenomenon known as "the wall."[21] Better "connecting the dots" between bits of information government already had might have prevented the attacks.[22]

---

[14] Office of the Director of National Intelligence, *Annual Statistical Transparency Report for Calendar Year 2021*, at 21 (released 2022).

[15] Office of the Director of National Intelligence, *Annual Statistical Transparency Report for Calendar Year 2024*, at 27 (released 2025).

[16] Joint Statement of ODNI, NSA, CIA, FBI, and DOJ, U.S. Senate Committee on the Judiciary, at 10 (June 13, 2013).

[17] *See* text accompanying note 1.

[18] Associated Press, *Lawmaker: Report shows FBI ignored accused Fort Hood shooter Nidal Hasan out of political correctness*, July 19, 2012, *available at* https://www.cbsnews.com/news/lawmaker-report-shows-fbi-ignored-accused-fort-hood-shooter-nidal-hasan-out-of-political-correctness/.

[19] Prepared Statement of Douglas Winter, Deputy Chairman, Webster Commission on Fort Hood Shootings, before the House Homeland Security Subcommittee on Oversight, Investigations, and Management (Sept. 14, 2012).

[20] Final Report of the William H. Webster Commission on The Federal Bureau of Investigation, Counterterrorism Intelligence, and the Events at Fort Hood, Texas, on November 5, 2009 (2009).

[21] *The 9/11 Commission Report*, National Commission on Terrorist Attacks Upon the United States (2004), at 79.

[22] *See id.* at 355-356 (text box).

Preventing investigators from querying existing holdings early in an investigation, when they likely lack probable cause, risks re-erecting the pre-9/11 "wall." How are agents supposed to discover relevant, unknown information in government holdings without running queries? If an FBI agent is investigating a person who appears to be radicalizing toward violence, and the government has 702 collection showing that that person communicated with an ISIS member overseas, we want the agent to discover that connection.

In one recent instance, such a query appears to have stopped a terrorist attack. The FBI revealed in 2024 that a U.S.-person query uncovered a connection between someone in the United States and a foreign terrorist group. The suspect "had acquired the means to conduct an attack and had already identified specific targets in the U.S."[23] The FBI was able to stop the plot within weeks of running the query.

Queries have also helped prevent "the potential illicit transfer of export-controlled technology that could be used in bioweapons production" and to disrupt a foreign government's attempt to dupe an American into handing over information about weapons of mass destruction.[24] The latter example also illustrates how queries, and intelligence collection generally, can help protect Americans from being harmed by foreign adversaries.

Requiring a court order will prevent queries just when they are most valuable: early in an investigation, before an agent is aware of the depth of a person's connection to a foreign threat. Stopping agents from finding those connections within the government's own holdings will make Americans less safe.

b. *U.S.-person queries are not a "backdoor" into Americans' private communications*

These queries are sometimes derided as "backdoor searches," a tautology which misstates both the legal and practical significance of these database checks.

To begin with, as a practical matter, a check of the 702 database is not remotely comparable to directly wiretapping an American or getting a warrant to collect the content of an American's stored messages. Section 702 collection itself is already limited to particular foreign targets: it *only* collects information to or from specific accounts or identifiers ("selectors") used by non-American, overseas foreign-intelligence targets. That already focuses the collection away from domestic communications and makes it unlikely that an American's routine messages would be swept up.

Of that already-focused collection, only a very small portion goes to the FBI. (As a domestically focused agency, its U.S.-person queries raise the greatest potentially privacy

[23] John Sakellariadis, *FBI reveals controversial spy tool foiled terror plot as Congress debates overhaul*, Politico, Feb. 13, 2024; *see also FISA Section 702 Value, supra*.

[24] *FISA Section 702 Value*, *supra.*

concerns.) The Bureau receives data only on a very small subset of targets: roughly 3 percent as of 2023.[25] Checking a 3% sliver of collection that is already tightly focused on foreign targets is hardly equivalent to gaining "backdoor" access to an American's email account or phone calls.

c. *The Government Does Not Need a Warrant to Check its Own Databases*

Some argue that the Constitution requires warrant for the government to run these database checks. It does not.

The U.S. Supreme Court has never held that investigators need a warrant to retrieve entries in a database that the government created and maintains. *Carpenter*, thus far the outer limit of Fourth Amendment case law on digital searches, involved compulsory process served on a private party, not a query of the government's own databases.[26]

One federal district court did recently hold that U.S.-person queries can require a warrant. In *United States v. Hasbajrami*, a judge in the Eastern District of New York reasoned that "the government cannot circumvent application of the warrant requirement simply because queried information is already collected and held by the government."[27]

That holding relied on *Riley v. California*, in which the Supreme Court held that police must obtain a warrant to search an arrestee's cellphone.[28] But *Riley* involved a physical "effect" that was unquestionably the property of the arrestee. The other cases cited by the district court similarly involved physical effects (computers, disks, and packages) that belonged to someone other than the government.[29]

U.S.-person queries, by contrast, involve a database created, owned, populated, and controlled by the government. The database may record private information, but the entries in the database are not an "effect" belonging to the communicants, who have no right to access, delete, or modify them. Nor can a private party assert a continued "reasonable expectation of privacy" in the contents of the 702 database. It is undisputed that the information in the database could have been lawfully examined by an analyst when it was initially collected under 702. Indeed, it is entirely possible that, for many queries, the responsive 702 information *already was reviewed* by the relevant analyst at the time it was collected. It would be anomalous to say that a

[25] *See* Williams and DiZinno, *supra*, at B-15. RISAA enshrined in statute the existing limits on the FBI's access to raw 702 data. *See* RISAA § 3(b) ("The Federal Bureau of Investigation may not ingest unminimized information acquired under this section into its analytic repositories unless the targeted person is relevant to an existing, open, predicated full national security investigation by the Federal Bureau of Investigation.").

[26] *Carpenter v. United States*, 585 U.S. 296 (2018).

[27] No. 1:11-cr-00623-LDH (Jan. 21, 2025).

[28] 573 U.S. 373 (2014).

[29] *Hasbajrami*, *supra* note 27, at 21-22.

person somehow regained a reasonable expectation of privacy in the text of an email at some point after it had already been lawfully collected and read by an intelligence officer.[30]

Thank you for the opportunity to testify today. I look forward to your questions.

[30] The court rejected this argument, calling it "akin to claiming that law enforcement can access privileged communications reviewed by a filter team because government employees laid eyes on the privileged communications at some point in the process." *Id.* at 25. But the two are not alike at all. A filter team's purpose is to prevent investigators from seeing or acting on the privileged communications. By contrast, an intelligence analyst reviewing 702 interceptions as they come across the transom is trying to do just that: find useful intelligence and act on it. The filter team and law enforcement are at cross-purposes by design; the initial analyst and the person who later runs the query are pursuing the same goal, just at different times.