Chairman Charles E. Grassley Questions for the Record
Professor Adam Klein
Strauss Center at the University of Texas at Austin School of Law
U.S. Senate Committee on the Judiciary
Review and Reform: The Foreign Intelligence Surveillance Act and Executive Accountability January 28, 2026

[Responses in blue Times New Roman font.]

Section 702 of the Foreign Intelligence Surveillance Act allows the government to conduct targeted surveillance of non-U.S. persons located abroad to acquire foreign intelligence information. Section 702 surveillance can acquire communications with U.S. persons if the surveillance target is in contact with them, but U.S. persons cannot be targeted by Section 702. The government's targeting, minimization, and querying procedures are all subject to judicial review by the Foreign Intelligence Surveillance Court and must be approved on an annual basis in order for the government to lawfully carry out the program.

1. **Please explain what it means to "query" information lawfully collected pursuant to Section 702 and why requiring a warrant for US person queries would be detrimental to national security.**

What is a query of 702 data?

A "query" is simply a digital check of information already held in government systems. A query is analogous to using the search bar in Windows, iOS, or Android to find contacts or files stored on a computer or phone.

Queries do not bring any new information into the government's possession. Instead, they simply retrieve information the government already has.

When an FBI agent queries 702 data, the queries run only on the FBI's holdings, which relate to roughly 3% of the overall targets.[1] The same limitation applies to the other intelligence agencies that receive collection from Section 702.[2]

Why are queries important?

Imagine that an FBI informant tips off the Bureau to a young man who has been talking fervently about ISIS, asking questions about religious martyrdom, and sharing online videos about buying weapons.

If information the government has already collected under Section 702 shows that the young man had previously been in contact with a known ISIS recruiter overseas, we would certainly want the FBI agent who is investigating the lead to know that. A query would alert the agent that the information exists in government holdings.

---

[1] *See* Klein Written Testimony at 9 & note 25.
[2] Office of the Director of National Intelligence, *Annual Statistical Transparency Report for Calendar Year 2024*, at 23 (2025).

At this point, our counterterrorism agent has enough information to take initial investigative steps.[3] But the agent does not yet have probable cause. No probable cause, no warrant.

The result: If a warrant were required, our agent would not be able to run the query. He would likely never learn that the young man had been in contact with an ISIS recruiter. He would not know that this lead—one among many on his plate—is an urgent threat. He might pursue it at a routine pace, instead of with maximum urgency. This could give the young man time to carry out a terrorist attack.

This is a sadly familiar pattern in 21st-century counterterrorism: after a devastating attack, we learn that investigators were "not made aware of and did not connect important details" that were already in the government's possession.[4]

9/11 and the Fort Hood massacre taught a clear lesson: counterterrorism investigators must have access to all information the U.S. government has already collected about their cases and the people involved. Failing to "connect the dots" leads to preventable terrorist attacks.

___

Most courts that have considered the issue have found that the querying of 702 information is not a Fourth Amendment-triggering event.

2. **If Congress were to impose a warrant on certain US person queries beyond what is required by the Fourth Amendment, what are measures that could be included to mitigate negative impacts to national security if Congress imposed a warrant requirement?**

Categorically excluding investigations related to national security from the court-order requirement.

___

Section 5(d) of the Reforming Intelligence and Securing America Act (RISAA) contained a clear mandate entitling certain members and their designated staff "to attend any proceeding"[5] of the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review. Yet the Department of Justice implemented procedures, including a "prioritization list" citing space concerns, limiting congressional access to hearings. The DOJ also seeks to limit congressional access to portions of Foreign Intelligence Surveillance Court and Foreign Intelligence Surveillance Court of Review proceedings despite RISAA's clear mandate.

3. **Why is congressional oversight of these proceedings important?**

---

[3] *See* United States Department of Justice, *The Attorney General's Guidelines for Domestic FBI Operations* 17-18.
[4] *E.g.*, United States Department of Justice, Office of Inspector General, *A Review of the FBI's Handling of Intelligence Information Prior to the September 11 Attacks*, ch. 5(I). (2004); *see also* William H. Webster Commission on The Federal Bureau of Investigation, Counterterrorism Intelligence, and the Events at Fort Hood, Texas, on November 5, 2009, *Final Report* (2009).
[5] *Reforming Intelligence and Securing America Act*, Pub. L. No. 116-49, § 5(d), 138 Stat. 862, 870 (2024).

Under our Constitution, Congress constitutes and funds lower federal courts, including the FISA courts.[6] To perform that constitutional role effectively, Congress must be able to form a detailed, accurate impression of how well the FISA courts are performing their statutory functions.

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 required transcripts of FISC proceedings, which would then be available upon request by the relevant congressional committees. I continue to support these reforms as a way to strengthen oversight and build trust in the FISA courts, particularly after the inadequate review of the applications to surveil former Trump campaign advisor Carter Page.

___

4. **Does the Department of Justice have the authority to restrict attendance, Foreign Intelligence Surveillance Court or Foreign Intelligence Surveillance Court of Review related information, and document sharing between Members of Congress and their designated staff?**

The FISA Court is not part of the Executive Branch; it is an Article III court.[7] While the Executive Branch has constitutional authority over security clearances and classification,[8] that does not extend to controlling access to Article III courts. The Executive Branch's authority to withhold classified information in criminal prosecutions, the closest plausible analogue, derives from a statute, the Classified Information Procedures Act, rather than some inherent constitutional power to control judicial proceedings that affect national security. Even the state secrets privilege, arguably the realm in which national security prerogatives intrude most aggressively into the normal functioning of the courts, requires that the court review and accept the government's assertion of the privilege.

---

[6] 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").

[7] *In re Sealed Case*, 310 F.3d 717, 731 (F.I.S.C.R. 2002).

[8] *Department of the Navy v. Egan*, 484 U.S. 518, 527 (1988). Members of Congress, however, are "cleared" for access to classified information by virtue of being constitutional officers, rather than by presidential grace. *Cf.* 50 U.S.C. § 3163.

To Adam I. Klein

1. Should the due process and Fourth Amendment protections guaranteed to U.S. citizens depend on executive branch compliance with internal manuals and administrative procedures? Why shouldn't Congress enact statutory safeguards?

   The protections guaranteed by the Due Process Clause and the Fourth Amendment do not depend on either Executive Branch practice or congressional enactments.

   Congress can, however, enact statutory safeguards that exceed those constitutional minimums.[1] In past writings and testimonies on this subject, I have supported many such safeguards.[2]

   Because safeguards above the constitutional floor are discretionary, the question is whether the benefit of imposing a given safeguard warrants any costs or risks it would impose.

2. In your testimony, you warned that requiring a probable-cause warrant could recreate the pre-9/11 "wall" between intelligence and law enforcement, risking another catastrophic terrorist attack. However, doesn't a warrant requirement simply impose judicial oversight and a probable-cause standard, rather than prohibit such queries altogether?

   Database checks are most useful early in an investigation, when investigators rarely have probable cause. For that reason, requiring probable cause to check government records will prevent agents from running those checks.

   Imagine that an FBI informant tips off the Bureau to a young man who has been talking fervently about ISIS, asking questions about religious martyrdom, and sharing online videos about buying weapons. The agent can take some initial investigative steps, but does not yet have probable cause. If information the government has already collected under Section 702 shows that the young man had previously been in contact with a known ISIS recruiter overseas, we would certainly want the agent to know that. But because he does not yet have probable cause, the agent would not be able to run the query.

3. You describe the privacy impact of U.S.-person queries as "modest." Given that these queries may access Americans' private communications without their knowledge or ability to challenge the search, how is that consistent with traditional Fourth Amendment protections?

---

[1] Hypothetically, there could be instances in which a desired statutory safeguard would impinge upon an exclusive constitutional power of the President. *Cf. Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 637-38 (1952) (Jackson, J., concurring).

[2] *See, e.g.*, Adam I. Klein, Chairman, U.S. Privacy and Civil Liberties Oversight Board, *Chairman's White Paper: Oversight of the Foreign Intelligence Surveillance Act* 6 (June 2021) (Summary of Recommendations); Adam I. Klein, Testimony before the U.S. House Committee on the Judiciary, Hearing on Section 702 of the Foreign Intelligence Surveillance Act 2-3 (March 1, 2017) (making numerous recommendations for statutory safeguards, many of which were subsequently enacted by Congress).

Queries of government records are fundamentally unlike search warrants or wiretaps of an American's private communications, which trigger traditional Fourth Amendment protections.

If it returns a hit, a U.S.-person query of stored 702 data pulls up a digital copy of a communication that was already lawfully intercepted by the government in the past and stored in a government database. The query brings *no new information* into the government's hands.

By contrast, search warrants and wiretaps pull in *new information that is not already in the government's possession.* Indeed, even forms of compulsory process that do not require probable cause—grand-jury subpoenas,[3] PR/TT orders, and 2703(d) orders—can pull in large amounts of previously uncollected personal information. Database queries pull in none.

4. In arguing that no warrant is required to query government-owned Section 702 databases, you distinguish cases such as *Riley v. California* by noting that the data is not a personal "effect." However, doesn't the reasonable expectation of privacy in personal communications persist even when those communications are stored in government databases—especially when they are initially collected without probable cause? Wouldn't querying Section 702 data therefore constitute a separate Fourth Amendment search, requiring independent justification?

   No. A private party cannot assert a continued "reasonable expectation of privacy" in information lawfully intercepted under Section 702 and copied into a government database. No one disputes that every single message in the database could have been reviewed by an analyst when it was initially collected under 702. Indeed, it is likely that, for many queries that return hits, the responsive message *was already reviewed* by an analyst at NSA, CIA, the National Counterterrorism Center, or the FBI at the time it was collected. It would be anomalous to argue that a person somehow regained a reasonable expectation of privacy in the text of an email at some point after it had already been lawfully intercepted, read by an intelligence officer, and saved in the government's files.

[3] *Cf. United States v. R. Enterprises*, 498 U.S. 292, 297 (1991) ("[T]he Government cannot be required to justify the issuance of a grand jury subpoena by presenting evidence sufficient to establish probable cause, because the very purpose of requesting the information is to ascertain whether probable cause exists.")

Senate Judiciary Committee
Hearing on
Review and Reform: The Foreign Intelligence Surveillance Act and Executive Accountability
January 28, 2026
Questions for the Record
Senator Amy Klobuchar

For Adam Klein, Director, Strauss Center for International Security & Law
University of Texas-Austin

The 2024 FISA reauthorization codified a number of measures that the FBI had implemented during the previous administration including requiring supervisory approval for U.S. person queries and batch queries. It also required the FBI's Deputy Director to personally sign off on sensitive queries like elected officials or media organizations.

- Do you believe that the current administration is complying with these Congressionally-enacted safeguards?

  I have not served in government since 2021, when I left my position as Chairman of the Privacy and Civil Liberties Oversight Board. As a private citizen, I do not have access to nonpublic information that would enable me to independently assess compliance.

  The only recent, publicly available assessment of which I am aware, by the Department of Justice Inspector General, found that "the FBI has implemented all of RISAA's querying reforms" and determined that "the number of noncompliant queries identified in NSD oversight reports has been reduced substantially post-RISAA."[1]

This administration fired or pushed out numerous FBI officials, including the FBI's most senior national security, counterterrorism, intelligence, and criminal and cyber response personnel.

- Are you concerned that these departures of key personnel make the Bureau less able to comply with the safeguards Congress put in place?

  As a private citizen, I do not have access to information that would enable me to form a non-speculative, informed judgment on internal personnel decisions within the FBI.

[1] U.S. Department of Justice, Office of Inspector General, *A Review of the Federal Bureau of Investigation's Querying Practices Under Section 702 of the Foreign Intelligence Surveillance Act* (Oct. 2025).

Questions for the Record for Adam Klein
Hearing on "Review and Reform: The Foreign Intelligence Surveillance Act and Executive Accountability"
Submitted February 4, 2026

QUESTIONS FROM SENATOR COONS

1. In your testimony, you argued that the Section 702 authority should be made permanent. What would you say to those who think that reauthorization votes provide necessary opportunities for Congress to make sure the authority is being used properly and to consider any necessary reforms?

   Reauthorization votes have provided useful opportunities to examine past use of FISA authorities and to consider reforms. At the same time, attaching a sunset to 702 creates the risk that it could lapse for reasons unrelated to the merits of the program. It is hard to imagine a scenario in which it would be prudent for the United States to forgo this valuable source of intelligence collection on priority foreign targets. Our enemies would gain room to maneuver, while Americans would face an increased risk of terrorist attacks, ransomware, foreign subversion of our electoral processes, and attacks on our troops abroad. Instead, Congress should use other mechanisms to ensure regular review of FISA authorities.

2. Do you think Congress should close the "data broker loophole" by which the government can circumvent restrictions by purchasing Americans' data directly from private companies that hold it?

   The widespread commercial availability of Americans' sensitive personal data is a risk to both privacy and national security. Once on the open market, it is difficult to prevent the data from making its way to adversarial foreign governments, fraudsters, and others who seek to use it to harm Americans. For that reason, in previous testimony before the Committee, I have supported buyer-agnostic regulations of data brokerage.[1]

   For data that remains commercially available, I do not support an outright ban on government purchases. There are legitimate governmental reasons to buy commercially available data, including defensive efforts to counter U.S. adversaries' use of the same datasets for targeting, phishing, and other malicious purposes. Limits on the government's use and handling of certain sensitive categories of commercially acquired data are less likely to impinge on legitimate uses.[2]

---

[1] *See* Testimony of Adam Klein before the U.S. Senate Committee on the Judiciary, Subcommittee on Privacy, Technology, and Law, *Protecting Americans' Data from Hostile Foreign Powers*, at 11 (Sept. 14, 2022) ("As long as [the data-brokerage] business model persists, it will remain virtually impossible to prevent this information—and the intelligence bounty that it represents—from falling into the hands of hostile foreign powers."), *available at* https://www.judiciary.senate.gov/imo/media/doc/Testimony%20-%20Klein%20-%202022-09-14.pdf.

[2] *See, e.g.*, ODNI Panel on Commercially Available Information, *Report to the Director of National Intelligence*, §§ 4.2-4.3 (Jan. 27, 2022), *available at* https://www.odni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf.

3. Should Congress reconsider—and if so, how—the provisions of the *Reforming Intelligence and Securing America Act* that:

    a. Expanded the definition of "foreign intelligence information" to include "international production, distribution, or financing of illicit synthetic drugs, opioids, cocaine, or other drugs driving overdose deaths"?

        No.

    b. Allowed agencies to use Section 702 queries to vet non-U.S persons being processed for travel to the United States?

        No. Our government should use all available information to ensure that those granted the privilege of visiting the United States mean us no harm.