To Elizabeth Goitein

From Sen. Lee

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?

3. Do you believe a probable-cause warrant requirement for U.S.-person queries under Section 702 is necessary to vindicate Fourth Amendment and separation-of-powers principles?

Combined answer to Questions #1 and #3:

The crux of the Fourth Amendment, reflecting the wisdom the framers gained through painful experience under British colonial rule, is the requirement of a warrant issued by a neutral magistrate. By requiring advance judicial approval of searches and seizures, the framers brought the separation of powers to bear in service of protecting civil liberties. They understood that the executive branch could never be "neutral" in defining and enforcing the limits of its own powers. As Chief Justice John Roberts put it in *Riley v. California*, a 2014 case holding that police officers need a warrant to search the contents of cell phones that are seized incident to arrest, "the Founders did not fight a revolution to gain the right to government agency protocols."

When government officials are not required to show probable cause to a neutral magistrate, it opens the door to abuse. Officials may conduct searches for impermissible purposes, such as targeting political enemies or spying on protesters. Searches are also much more likely to be infected by racial, ethnic, religious, or ideological bias, whether conscious or subconscious. These risks have materialized in the context of warrantless Section 702 queries, which have included improper searches for the communications of members of Congress, protesters from across the ideological spectrum, and "Middle Eastern" men.

Even if the motive of the searching official is entirely legitimate — e.g., to discover evidence of criminal activity — the absence of a warrant requirement enables fishing expeditions, in which Americans are subjected to intrusive searches without any evidence that they are engaged in wrongdoing. Such fishing expeditions were known as "general warrants" in colonial times; they were the primary impetus for the Fourth Amendment and one of the driving forces behind the revolution itself. Yet they appear to be standard practice for Section 702 queries: Government officials acknowledge that agents usually perform queries at the earliest stages of an inquiry, when they may have very little information about the foreign threat they are investigating — let alone evidence of the U.S. person's involvement.

Courts have never previously been confronted with a situation in which the government "incidentally" obtains massive amounts of Americans' private communications without a warrant and then seeks to locate and retrieve that information from within its databases. The issue is now working its way through the regular federal courts. (Unsurprisingly, the Foreign Intelligence Surveillance Court, which has historically shown extreme deference to the government, has approved the warrantless searches.) Most recently, after the Second Circuit Court of Appeals unanimously rejected the government's argument that the Fourth Amendment

places no restrictions on searches of lawfully acquired information, a district court held that U.S.-person queries are subject to the Fourth Amendment's warrant requirement.

Congress, however, should not wait for further judicial action. Courts are often slow to respond to novel Fourth Amendment scenarios, and they have occasionally stumbled in their initial responses. In 1928, for instance, the Supreme Court held that the government's wiretapping of telephone calls did not implicate the Fourth Amendment if it did not result in a property intrusion. It took almost 40 years for the Court to reverse the holding, affirming that the Fourth Amendment protects privacy, not just property. Congress should thus act now to codify Fourth Amendment protections by requiring government officials to obtain a probable-cause court order before accessing Americans' communications obtained under Section 702.

2. During the hearing, you highlighted the FBI's repeated failure to fully track U.S.-person queries as required by law, resulting in incomplete compliance data for 2024 and 2025.

    a. Do these tracking failures undermine confidence in the effectiveness of the 2024 RISAA reforms?
    b. How would requiring a probable-cause warrant for these queries strengthen accountability and reduce the risk of abuse?

As detailed in my testimony, the National Security Division (NSD) discovered in August 2024 that the FBI was using a tool known as an "advanced filter function" to query information obtained under Section 702. Even though the FBI used this tool to search for and pull up the communications of specific individuals, including U.S. persons, it inexplicably chose not to consider these searches "queries." As a result, U.S.-person queries conducted using this tool were not tracked, counted, or audited as required by law. Moreover, FBI agents likely failed to obtain attorney approvals for U.S.-person queries, another requirement imposed by RISAA. The NSD acknowledged that FBI agents may have run sensitive queries without the statutorily required supervisory approvals and may have violated RISAA's prohibition on evidence-of-a-crime-only queries.

In short, the FBI systemically violated multiple statutory requirements for an unknown period of time. Needless to say, this fact does not give confidence that the FBI is faithfully interpreting and applying other provisions of RISAA. Nor should members of Congress draw much comfort from the fact that the NSD discovered and reported the violations. For one thing, there is no public information on how long the FBI was engaged in this practice before the NSD discovered it. Moreover, after the discovery, the NSD apparently took several months to determine whether these searches of Section 702 data were queries — a delay that raises concerns about the NSD's own stewardship. Perhaps most concerning, the FBI's conduct raises questions about other ways, not yet detected by NSD, in which the FBI might be attempting to evade RISAA's constraints through disingenuous interpretations of the term "query" or other means.

A warrant requirement for U.S.-person queries would not directly address the problem of the FBI deciding not to treat certain searches as queries. But it would address other compliance concerns that are heightened by the FBI's continuing pattern of violations. In particular, a warrant requirement would go far toward ensuring that agents do not access U.S. person information for

improper purposes or as part of a fishing expedition. To prevent the FBI from evading a warrant requirement through specious interpretations of the term "query," however, Congress must amend the existing statutory definition of that term to more clearly and comprehensively and specify the actions it encompasses.

4. Some argue that a warrant requirement would delay or hinder national security operations.

    a. Are there any categories of U.S.-person queries that would become impossible under a probable-cause warrant requirement?
    b. Do you believe the government could still effectively protect national security if such a requirement were adopted?

Existing warrant proposals would generally require government officials to obtain a warrant or FISA Title I order before accessing communications content or other Fourth Amendment-protected information retrieved through U.S.-person queries, with exceptions for consent, exigent circumstances, and defensive cybersecurity purposes. Other than queries conducted for the sole purpose of returning evidence of a crime — which Congress already has prohibited — there are no categories of U.S.-person queries that would be off limits under these proposals. The only foreign intelligence queries that would become impossible to conduct are those that were neither supported by probable cause nor justified under one of the exceptions. Government officials would thus be unable to conduct searches to target political enemies; spy on protesters and journalists; investigate individuals based on constitutionally protected characteristics, such as race, religion, or political affiliation; or engage in fishing expeditions without evidence.

Opponents of this reform nonetheless claim that a warrant requirement could harm national security. In asserting the national security value of warrantless searches, they rely heavily on generalizations, hypotheticals, and conjecture. But there is no need to speculate; Section 702 has an 18-year track record. As part of its comprehensive review of the program in 2023, the Privacy and Civil Liberties Board examined classified and unclassified information about the FBI's U.S.-person queries over a period during which these queries were particularly numerous. The Board concluded that "there was little justification provided to the Board on the relative value of the close to 5 million searches [U.S.-person queries] conducted by the FBI from 2019 to 2022." The government cited some instances in which U.S.-person queries had been useful in identifying and warning victims of attacks, but as the Chair of the Board noted, the government may obtain consent or invoke the exigent circumstances exception in such cases.

Of course, there is no way to rule out a future hypothetical situation in which liberty and security come into tension. Reconciling these considerations is the core function of the Fourth Amendment. The balance the framers struck was that the government may intrude on Americans' privacy rights, with all the risks such intrusion entails, if it can show probable cause to a neutral magistrate. This balance has protected both our nation and our liberties for 250 years; Congress should reaffirm it now.

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 Elizabeth Goitein, Senior Director, Liberty & National Security Program
Brennan Center for Justice

In 2024 during the last FISA Section 702 reauthorization cycle, concerns were raised that if Congress allowed Section 702 authorities to lapse, the Intelligence Community could try to "backfill" the information gap by using Executive Order 12333 authorities which are less privacy protective.

In your written testimony you noted that the distinction between FISA authorities and E.O. 12333 authorities "has critical consequences, as there are exceedingly few legislative protections for Americans' privacy when the government conducts surveillance under E.O. 12333."

- *Do you share the concern that the Intelligence Community would attempt to backfill the information gap caused by FISA Section 702 lapsing by reverting to less privacy protective authorities?*

If Section 702 were to expire, the Intelligence Community (IC) would certainly seek to backfill the resulting information gap through other means, including through acquisition under Executive Order 12333. In practice, the IC would likely be able to use these workarounds to acquire some, but not all, of the same general information.

One constraint would be FISA's "exclusive means" directive. If Section 702 were to expire, the rest of FISA would remain in place — including the provision stating that FISA and the criminal code "shall be the exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted." 50 U.S.C. § 1812. Much of the collection that currently takes place under Section 702 meets the statutory definition of "electronic surveillance," and so it would have to take place under other parts of FISA. In some circumstances, the acquisition of communications content could only occur under Title I, which would require a showing of probable cause that the foreign target was either a foreign power or an agent of a foreign power.

The definition of "electronic surveillance," however, is badly out of date, as it is keyed to methods and technologies — for both communication and acquisition — that existed decades ago. The result is significant gaps in coverage. For instance, the definition covers wire communications to and from U.S. persons only if the acquisition takes place in the United States, and it covers "radio" communications only if the sender and all recipients are located in the United States. It does not cover wiretaps conducted overseas or the acquisition of wireless international communications.

Moreover, "electronic surveillance" is defined as the acquisition of information through "an electronic, mechanical, or other surveillance device," because that was how the government obtained communications before the advent of emails and text messages stored with third-party service providers. Although the government appears to treat the collection of stored communications as "electronic surveillance," the definition itself leaves far too much wiggle room on this point.

Finally, while Section 702 authorizes the collection of any type of information, "electronic surveillance" applies only to the acquisition of communications content or other information subject to Fourth Amendment protection. In the digital era, people's daily activities generate a wealth of data (such as geolocation information) that can be collected and crunched to reveal information every bit as sensitive as communications content. Because the acquisition of this data does not meet the definition of "electronic surveillance," it could continue under Executive Order 12333 if Section 702 were to expire.

Executive Order 12333 does not itself create a mechanism by which the government may obtain a court order requiring companies to turn over information. Accordingly, the government would need to identify another available form of compulsory process; conduct surveillance directly (e.g., through overseas wiretaps); rely on voluntary cooperation by companies that store the information; or purchase the information from those companies or from data brokers. These practical constraints are not insignificant, but they would still leave the government with multiple sources of access.

In short, the expiration of Section 702 could make the acquisition of some types of information more difficult and costly, and it could preclude the collection of some information altogether (e.g., certain acquisitions of communications content where the target is not a foreign power or agent of a foreign power and the communications can only be obtained through "electronic surveillance"). However, other categories of information currently obtained under Section 702 could be obtained through other means — including through activities under Executive Order 12333, which operates without statutory protections for Americans, transparency, or judicial oversight.

Of course, the solution here is not to simply reauthorize a law that fails to protect Americans' privacy, lest the government turn to an authority that is even *less* protective. The solution is twofold. First, Congress must reform Section 702 to include sufficient protections for Americans, including a requirement that government officials obtain a warrant before combing through Section 702 to find Americans' communications. Second, as discussed on pages 37-38 of my written testimony, Congress must legislate basic protections for Americans whose constitutionally protected information is acquired under Executive Order 12333.

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

QUESTIONS FROM SENATOR COONS

1. *I am proud to co-lead the NDO Fairness Act with Senator Lee, a bill that would reform the process for obtaining non-disclosure orders (NDOs) by imposing more exacting standards and heightened requirements before NDOs can be issued by courts. Although this bill is not directly related to FISA Section 702, the government's use of NDOs when seeking electronic records from online platforms prompts similar issues at the intersection of law enforcement and personal privacy.*

    a. *Are you familiar with the practice of federal government officials obtaining an NDO prohibiting an electronic communications service provider from notifying the subject of a warrant about the government's request? If so, do you believe that practice should be reformed?*

    b. *Do you believe that an individual should be given notice that his data has been seized by the government when doing so does not jeopardize an investigation?*

My answer to all three questions is yes, and I commend your leadership in working to address this worrisome practice.

For many types of searches and seizures, the government is required by law to notify the target. For instance, the government must provide the target of a physical search with the copy of a search warrant, along with an inventory of property seized, and it must notify targets of wiretaps within 90 days of the end of surveillance (although the notice may be postponed for good cause). This requirement of notification is a critical protection for Americans' constitutional rights. Put simply, Americans cannot challenge unconstitutional searches or surveillance or hold the government accountable for unlawful practices if they do not know these actions have occurred.

Despite the importance of notification, the law permits the government to engage in certain types of acquisition of sensitive information — often involving the collection of information from third parties, such as electronic communications service providers — without providing notice to the target. Moreover, even when notice is required, it is far too easy for the government to obtain indefinite postponements, effectively negating the requirement.

Compounding this problem, current law permits the government to obtain gag orders (known as "non-disclosure orders," or NDOs) that prevent third-party service providers from notifying customers whose information has been subpoenaed or otherwise acquired by government agencies under the Stored Communications Act. Although the bar for issuing these orders should be high — courts are required to grant them only if notification would cause certain enumerated harms or would seriously jeopardize the investigation — companies report that the orders have become commonplace. Many are based on boilerplate allegations and findings rather than

specific facts. And because there is no statutory limit on the duration of these orders, they are often indefinite, remaining in place long after notifying the customers could cause any harm.

The NDO Fairness Act would make significant inroads into this problem. It would require courts to issue written determinations, based on specific and articulable facts, that one of the harms cited in current law would result from notification; that the order is narrowly tailored; and that there is no less restrictive alternative than the order being issued. It would limit the initial duration of most orders to 90 days, with 90-day extensions available only upon written determinations by the court that the statutory criteria continue to be met. It would give service providers the right to contest NDOs in court. And it would generally require the government to notify the target of collection upon expiration of an NDO.

These reforms would go a long way toward addressing a discrete problem: the use of NDOs to prevent notification of targets when the government acquires information under the Stored Communications Act. Further reforms are needed, however, to address the larger problem of Americans being kept in the dark when the government obtains their sensitive information. For one thing, while many companies would choose to notify customers absent a gag order, other companies do not provide such notice even when they are free to do so. In particular, many telephone companies do not have policies of providing notice to their customers. Moreover, there are forms of surveillance that do not necessarily involve third parties and that may take place without notification — or with indefinitely delayed notification — to the target.

To solve this wider problem, and as a complement to the NDO Fairness Act, Congress must bolster requirements for the government to notify the targets of searches or surveillance in cases that do not involve NDOs. Congress could accomplish this through legislation along the lines of the Government Surveillance Transparency Act, a bipartisan bill introduced in the 117th Congress by Senators Wyden, Daines, Lee, and Booker.