Statement of Gene Schaerr
General Counsel, Project for Privacy & Surveillance Accountability
and Managing Partner, Schaerr | Jaffe LLP

Before the House Judiciary Committee
Hearing on "Oversight of the Foreign Intelligence Surveillance Act"
Dec. 11, 2025

Chairman Jordan, Ranking Member Raskin, and members of the committee, thank you for holding this timely and important hearing on oversight of the Foreign Intelligence Surveillance Act (FISA).

As you know, a key FISA authority – Section 702 – is up for reauthorization in April. That authority, enacted by Congress to surveil foreign threats on foreign soil, has become a major means by which the federal government warrantlessly spies on American citizens on American soil. Where that program stands today, and what we know about its development into a major domestic spying tool, I will get to in a moment. But first I want to step back and explore what this development tells us – namely, that surveillance authorities tend to metastasize over time, moving from legitimate purposes to less legitimate ones.

The expansion of surveillance is driven in part by men and women in the Intelligence Community who are passionate about their mission to protect the American people and our homeland. Their patriotism and service deserve our appreciation. But surveillance expansion is also driven by the temptations of power created by increasingly robust technologies that increasingly allow agencies to peer into the lives of Americans.

It is for that reason that the last Section 702 reauthorization in 2024 became a wide-ranging debate over the growth of the surveillance state in America. That debate resulted in the passage of the Reforming Intelligence and Securing America Act (RISAA). RISAA was a great first step toward reform, but more is needed to guard against warrantless intrusions by government agencies into Americans' personal information and lives.

The Scope of the Surveillance State

Congress, appreciating how much is left undone, wisely put a two-year time frame on the 2024 Section 702 reauthorization. You thereby opted for a second opportunity to examine and correct the growing imbalance between government practice and Americans' constitutional rights and privacy interests.

Let us therefore briefly review four current Section 702 surveillance issues that require congressional attention if you, the People's representatives, are to prevent the creation of a full-blown American surveillance state.

- Despite the reforms of RISAA, Section 702 queries of Americans still do not require a warrant. Such queries enable government personnel to conduct "backdoor searches," circumventing the need for court approval before government agents seek out and read Americans' communications.

- Federal agencies, ranging from the FBI to the Department of Homeland Security to the IRS, routinely purchase Americans' sensitive personal digital information from shadowy data brokers. This data can include electronic records, communications metadata, web browsing activity, transaction and purchase records, online search, and many other forms of data that reveal Americans' most intimate beliefs, activities and associations. This data is far more personal than what can be gathered by hand, found in a diary, or pulled from a public website.

- Next is what I call the "make everyone a spy provision" in RISAA. The expanded Electronic Communications Service Provider (ECSP) provision, added in the eleventh hour during the last debate over surveillance in 2024, obligates providers of free Wi-Fi to customers to respond to secret requests by the National Security Agency for private communications. The law allows the government to force providers of office space to, among others, media, law firms, and political campaigns to facilitate warrantless surveillance of people

using their buildings' internet systems. There is nothing to prevent such spying from even being demanded of churches and other houses of worship.

- The addition over the years of amici to proceedings of the FISA Court also provides a much-needed window into civil liberties issues arising from the operations of that secret court. However, amici are still overly restricted in their ability to access critical materials and proceedings. There is also no amicus provision for FISA Title I surveillance, which can also turn a provision originally aimed at foreign threats into an authority for domestic spying.

That was most obviously true in the case of Carter Page, whom I am currently representing on appeal. As you know, he was illegally surveilled by the FBI as a means of spying on a presidential campaign and transition. The four warrants issued by the FISA Court to spy on Mr. Page – none of them examined by an amicus – were, as the Department of Justice Inspector General has established, predicated on a political opposition research document whose most lurid story turned out to be a bar joke. When the Court asked the FBI if Mr. Page had been an asset of the CIA – which he was – an FBI attorney submitted a forged document to the Court saying he was not.

Regardless of party, all members of Congress should be alarmed by this – by an Intelligence Community that asserts the right to interfere in a presidential election in such a dishonest and disingenuous way.

In addressing these four specific needs for FISA 702 reform, Congress should also bear in mind other important developments that are steadily contributing to the development of an American surveillance state.

- For example, when Americans travel through airports or malls, or even walk down a city sidewalk, we are subject to being identified and tracked by their faces. Cell-site simulators in geofenced areas also ping our phones to follow our movements. Our automobiles keep a record of every place we drive – and license plate readers create a database of our movements. Upon our return to U.S. international

airports, our digital devices are subject to having all their contents downloaded and inspected without a warrant.

- All this data generated from myriad sources can then be woven together by the power of artificial intelligence to comprehensively track where we go, who we meet with, what we say or share in private, and what we believe.

- As a result, federal agencies are capable of generating comprehensive political, religious, romantic, health, and personal dossiers on every American from information gathered without a warrant. That is as about as far from James Madison's Fourth Amendment as one can imagine. And it is an additional compelling reason to insist on meaningful Section 702 reforms.

RISAA's Reforms Were Not Enough

As I mentioned earlier, chief among the needed reforms is additional guardrails on warrantless "backdoor searches" of Americans' communications in the Section 702 database. The FBI in 2021 conducted more than 3 million of these searches, an astonishing abuse of a surveillance power that Congress designed for *foreign surveillance*, not warrantless surveillance of Americans.

Further, according to several FISA Court opinions, the FBI frequently has conducted those backdoor searches in politically sensitive cases. For example, in violation of its own rules, the FBI a short time ago illegally searched for communications of 19,000 donors to a congressional campaign, of multiple U.S. government officials, of journalists, of political commentators, of a local political party, of people who came to the FBI to perform repairs, of victims who approached the FBI to report crimes, of business, religious, and community leaders who applied to participate in the FBI's "Citizens Academy," of college students participating in a "Collegiate Academy," of police officer candidates, of colleagues and relatives of FBI agents, and of Black Lives Matter and January 6 protesters.

Defenders of the status quo will claim that passage of RISAA closed the loopholes that allowed such abuses. And no doubt, on the whole, RISAA was an important and valuable step forward. Congress strengthened oversight and codified the rules and procedures the FBI itself had adopted in late 2021 and early 2022. These rules and procedures were meant to prevent the misuse of searches in sensitive cases that involve Americans' most basic civil rights and political expression.

Yet some of the most egregious improper queries *occurred after* the FBI's new rules were implemented. In April 2023, a FISC opinion revealed that the FBI in 2022 dipped into Section 702 data to warrantlessly spy on a United States Senator, a state senator, and a state judge who had the temerity to report suspected civil rights violations by a local police chief.

As these abuses continue, the legal foundation for warrantless searches of Americans is under challenge.

In 2024, a federal district court in New York ruled that the government violated the Fourth Amendment when it failed to obtain a warrant before it conducted such a "backdoor search" in a criminal case using data derived from Section 702.[1] But this is far from settled law. As we have seen repeatedly, a judicial ruling here or there has proven insufficient to deter warrantless searches.

And besides, protecting Americans' privacy is primarily the role of Congress, not the judicial branch. It will take Congressional action – making full use of the coming Section 702 debate – to achieve lasting reforms that protect Americans' privacy and curtail the growing surveillance state.

Section 702: What Remains to be Done

What, specifically, should Congress do now? Remember first that Congress originally intended Section 702 to be limited to the communications of foreigners, an appropriate authority in a time of geopolitical tension. But because Americans are often in communication

[1] *United States v. Agron Hasbajrami*, U.S. District Court for the Eastern District of New York, Dec. 2, 2024.

with people outside the United States, and because of the interconnected nature of global communications systems, surveillance under Section 702 inevitably sweeps up vast amounts of Americans' communications.

Absent Congress's mandating a warrant requirement for searches for Americans' communications in the 702 database, significant abuses will inevitably occur. We should be very concerned about any framework that allows the FBI to routinely search through Americans' communications without a warrant.

That isn't to say the warrant requirement must be absolute or inflexible. The Intelligence Community's own testimony during the last reauthorization offered only a few scenarios in which U.S. person queries – the warrantless searching of Americans' communications in the Section 702 database – had significant value. And the warrant rule proposed by this Committee included reasonable exceptions that would allow the government to act effectively in every exceptional circumstance.

Despite these reasonable compromises, the Intelligence Community is still obfuscating, perhaps in defiance of clear mandates from Congress. The DOJ Inspector General reports that, from December 2023 to November 2024, the number of U.S. person queries conducted by FBI personnel fell to 5,518 – from a high of more than 852,000 in 2019 to 2020.

That sounds like tremendous progress. But on page 49 of the Inspector General's report, the OIG notes that auditors found that the system's "advanced filter functions" may allow for searches of targets' communication without counting them as "queries."[2]

I recommend this as an area for further investigation on your part. As you do, keep in mind that the Intelligence Community cannot have it both ways.

- If the advanced filter function is disguising to a significant degree the actual number of U.S. person queries, then RISAA may not have made as much progress as we had hoped.

[2] https://oig.justice.gov/sites/default/files/reports/26-002_0.pdf

- If, on the other hand, the current reported number is close to the actual number of U.S. person queries, then a requirement for a probable cause warrant for such queries should be a light burden, especially with all the exceptions that were built into this Committee's last 702 reform proposal.

Either way, the facts argue for Congress to impose a clear probable cause warrant requirement for ordinary Section 702 queries of Americans.

Your Achievements

In so doing, you can build on prior successes. In the last Section 702 debate, for example, you demonstrated that it is possible to set guardrails to protect Americans' civil rights against surveillance abuses. You showed that reform is possible while also ensuring that agencies have the ability to track and respond to genuine threats. In fact, on a nearly unanimous, bipartisan basis, this Committee marked up and approved the strongest surveillance reform legislation that we have seen in over a generation—showing your dedication and resolve to protect Americans' civil liberties.

While this Committee's bill was not ultimately adopted by the full Congress, it is still inspiring to consider what the 118th Congress did accomplish on surveillance reform:

- In the 118th Congress, you mandated that the FBI produce quarterly reports on the number of U.S. person queries conducted under Section 702, giving Congress real-time guidance.

- You cracked open the door of the Foreign Intelligence Surveillance Court to your oversight, allowing key Members with oversight responsibility to sit in on hearings – although we understand that provision may need to be strengthened further.

- You shortened the reauthorization of Section 702 from five to two years.

- And on the House floor, you came within a single vote – on a 212-212 tie – of requiring a warrant for the government to search Americans' communications in the Section 702 database.

Finally, last Congress the House also took a significant step in passing a measure to require warrants when federal agents purchase and inspect Americans' most intimate digital data – including their geolocation, internet search history, and online communications – sold to the government by data brokers with no regard for Americans' Fourth Amendment right to privacy.

Although these two warrant requirements did not ultimately become law, the progress made last Congress was a significant achievement, and we applaud this Committee for working to build on last year's strong bipartisan efforts to protect Americans' civil rights.

What You Can Achieve in 2026

Each of these reforms can be passed by this Committee and by Congress in 2026.

- You can take the lead by passing a warrant requirement for Section 702 searches of US persons' communications.

- You can also add a warrant requirement to the federal government's purchase and review of Americans' sensitive personal data.

- You can curb the definition of "electronic communication service provider" under FISA to exclude houses of worship and countless small businesses from being forced by the NSA to assist in spying on congregants and customers.

    - On that point: It has been widely reported in the media – and suggested on the floor of the United States Senate – that the dramatic expansion last year of the definition of "electronic communication service provider" was enacted in order to cover

data centers. We urge you to appropriately tailor the definition to achieve that purpose, but to go no further.

- Beyond that, you can require amici participation in sensitive political FISA cases by including the so-called “Lee-Leahy Amendment” in next year’s reauthorization. – which mandates the inclusion of a qualified civil liberties expert holding a high-level clearance to advise the secret FISA courts. This measure, which passed the Senate in 2020 with 77 votes, would go a long way to preventing the types of abuses that occurred in 2016 when the Trump campaign and transition was illegally spied based on improper FISA warrants that issued as a result of the FBI’s lies. The measure is popular because it makes so much sense to have at least one advocate for civil liberties in these secret hearings.

As you reform these practices, you can rest assured that the American people are behind you. A YouGov poll from 2023 shows that 76 percent of Americans support a warrant requirement for government inspection of Americans’ international communications. Eighty percent believe Congress should pass a law requiring a warrant before the government can purchase and access our digital data. As the debate on the reauthorization of Section 702 begins, you can speak and act with confidence, knowing that your constituents will be strongly on your side.

Expect Intelligence Community Curveballs

In approaching this debate, please also understand just how hard the Intelligence Community will work not just to stop future reforms, but to derail the reforms you’ve already made.

To cite one example, consider the RISAA reform that allows select Members of Congress and designated staff to attend the secret FISA hearings. This was intended to enhance oversight of the FISA courts and to put a check on judges who have sometimes shown astonishing naiveté in accepting the FBI’s assurances at face value.

A recent development in this story, however, shows just tricky it can be to deal with the Intelligence Community. Your Senate counterparts, Chairman Chuck Grassley and Ranking Member Dick Durbin, have publicly challenged Department of Justice rules setting limits on what you can access in FISC proceedings. The new DOJ procedures:

- Prohibit you from sharing information from these hearings with other Members or your cleared staff.

- Restrict you from requesting information or documentation from FISC proceedings.

- Allow DOJ staff to remove you from FISC proceedings for any reason.

- Prohibit you from bringing your designated staff member with you.

- Prohibit note-taking.

These measures mean that, if you attend a secret hearing and learn something that you want to discuss with another Member who had a right to attend the hearing, you will instead be effectively gagged from discussing it with each other or with any of your staff, regardless of security clearance or whether that discussion takes place in a SCIF.

So give them credit – DOJ found a way to turn your oversight and accountability measure into yet another mechanism for silencing you. But I am sure you agree that it is *Congress* that should spell out the rules for your access to oversight, not the very bureaucrats you oversee.

Along similar lines, it has recently come to light that former Special Counsel Jack Smith relied, not on a probable cause warrant, but on a grand jury subpoena, to examine the telephone metadata of eight U.S. Senators and one Member of this House. That is the very definition of a fishing expedition – one in which even Members of Congress are subject to exploratory

spying without the pretense of probable cause. And it should not be allowed.

Expect too to hear whispers that, if you press too hard for reform, you will be setting yourselves up to be responsible for the next 9/11. That is nonsense. As the 9/11 Commission report found, the nation's greatest modern intelligence failure resulted from an inability of siloed intelligence agencies to connect dots that had already been lawfully obtained. The reforms I have discussed today need not result in any such siloing of insights or information. We can protect our constitutional right to privacy while taking great care to make sure the Intelligence Community retains the exceptions and authorities it needs to keep America safe.

Conclusion

In sum: Revulsion at government surveillance runs deep in our DNA as a nation; indeed, it was one of the main factors that led to our revolt against British rule and, later, to our Bill of Rights. Agents of the Crown could break into a warehouse or a home to inspect bills of lading or secret political documents, but they couldn't access anything close to the wealth of private information reflect in our digital lives today.

Month by month, it is harder to square this emerging surveillance state with the "consent of the governed" concept articulated in the Declaration of Independence and embodied in Article I of the Constitution. The Founders believed that American citizens should not be subject to surveillance by their own government without their consent – in the form of a statute duly enacted by their representatives in Congress. They should not be subject to surveillance at the whim of any executive official, none of whom has authority to consent to surveillance on their behalf.

But decades of neglect and dismissal have tarnished that inheritance with intelligence practices that are self-justifying and self-serving. We look forward with hope that you will restore, protect, and burnish these privacy-protecting traditions of a free people.