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

Before the House Judiciary Committee
Subcommittee on Crime and Federal Government Surveillance
Hearing on:
"A Continued Pattern of Government Surveillance of U.S. Citizens"

April 8, 2025

Chairman Jordan, Ranking Member Raskin, Chairman Biggs, Ranking Member McBath, and Members of the Subcommittee, I thank you for examining the massive growth of government surveillance of Americans, and what can be done about it.

The Problem

We have seen under administrations of both parties the expansion of myriad forms of privacy-destroying technologies and practices—elements of an emerging American surveillance state being knitted together before our eyes.

Like the proverbial frog unaware that it is slowly being boiled alive, Americans are being progressively trapped in a system of national surveillance. This is not happening because federal agencies are run by tyrants. The men and women in the intelligence community are passionate about their mission to protect the American people and our homeland. But in their zeal to execute their important mission, they are rapidly creating the elements of a pervasive American surveillance state. And astonishingly fast changes in technology are helping build this surveillance state before our laws can catch up to keep it within the constraints of our Constitution.

At airports, at malls, on the streets, we are identified and tracked by our faces. Cellsite simulators in geofenced areas ping our phones to follow our movements. Our automobiles keep a record of every place we drive. Our digital devices at international terminals are subject to having all their contents downloaded and inspected without a warrant. Moreover, thanks to purchases of Americans' digital information from data brokers, federal agencies ranging from the FBI to the IRS, Department of Homeland Security, and the Department of Defense, routinely access, without a warrant, digital information far more personal than what can be gathered by hand or found in a diary. To top it off, we also face the routine collection of Americans' communications "incidentally" caught up in the global data trawl of programs authorized by Section 702, and in the past few years alone the FBI has conducted hundreds of thousands of warrantless searches of the Section 702 database specifically looking for Americans' communications.

The end result is that the government is now able to collect and search through vast amounts of Americans' communications and other personal data with ineffective statutory limits and limited congressional oversight. The personal data thus obtained reveals much about our health, mental health, and personal relations. Worse, all this

data generated from myriad sources can then be woven together by the instant 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.

This is as about as far from the Founders' vision of the Fourth Amendment as one can imagine. 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 a secret political document, but they couldn't access anything close to the wealth of private information contained 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. How does that principle apply today to surveillance reform?

The Importance of Warrants

Of course, there is a legitimate need in a dangerous world for the government, in some rare situations, to seize Americans' papers and other assets to search for threats to life and liberty. But the Founders recognized that this authority was in itself a great danger, perhaps one as great as any external threat. So they placed a boundary around this power with the Fourth Amendment's requirement for a warrant.

Warrants force government agents to justify their snooping with statements of probable cause. After the fact, warrants provide a paper trail that helps deter the government from invading Americans' privacy when there is no good reason to do so—that is, when there is no "probable cause" to believe any harm is being or is about to be inflicted on the Nation or one of its citizens. And that probable cause requirement should apply, not just to direct surveillance like tapping someone's phone or following them from place to place. It should also apply to more indirect forms of surveillance like searching a database of purchased information, or searching the massive trove of information compiled under Section 702 of FISA.

Yes, surveillance under Section 702 is in theory limited to foreigners' communications. But because Americans are often in communication 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. As the FBI admits, it sometimes conducts warrantless "backdoor searches" of those communications and other data in ordinary domestic criminal cases, and believes it has the right to do so routinely.

Further, according to several FISA Court opinions, the FBI frequently conducts those backdoor searches in politically sensitive cases. For example, in violation of its own rules, in just the last few years the FBI has searched for communications of Black Lives Matter and January 6 protesters, of 19,000 donors to a congressional campaign, of multiple U.S. government officials (including at least one member of this House), of journalists, political commentators, and a local political party, not to mention people who came to the FBI to perform repairs; victims who approached the FBI to report crimes; business, religious, and community leaders who applied to participate in the FBI's "Citizens Academy"; college students participating in a "Collegiate Academy"; police officer candidates; and colleagues and relatives of FBI agents.

Defenders of the status quo will claim that last year's passage of the Reforming Intelligence and Securing America Act (RISAA) in April 2023 closed the loopholes that allowed such abuses. As useful as RISAA was, that is far from the truth. What Congress did there was mainly to strengthen oversight and codify 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.

But the FBI failed even by its own procedural standards when it conducted over 204,000 warrantless searches for Americans' communications in the FISA database in 2022. A DOJ National Security audit recorded a "noncompliance" rate of 1.7 to 4 percent for such queries for that year alone. Even at the low-end estimate, that failure rate equals about 3,400 civil rights violations a year according to the FBI's own standards, almost 10 violations per day. Not to mention that all 204,000 of those searches sidestepped the Fourth Amendment and invaded Americans' privacy without probable cause or a warrant.

Some of the most egregious improper queries also occurred after the FBI's new rules were implemented. Even then, the FBI managed to dip 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. Moreover, since the passage of RISAA in April 2024, the Office of the Director of National Intelligence has revealed further improper searches of the communications of a congressional candidate, a chief of staff of a Member of Congress, U.S. government employees, and the spouse of an applicant for a security clearance.

As abuses continue, the legal foundation for warrantless searches is collapsing. In December, a federal district court 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.[1] That decision was based on an earlier decision by the influential Second Circuit holding that a government search of the Section 702 database is in fact a "search" for Fourth Amendment purposes.

As we have seen repeatedly, however, a judicial ruling here or there has proven insufficient to deter warrantless searches. Absent an explicit law mandating a warrant

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

requirement, such abuses will inevitably continue. We should be very concerned about any framework that allows the FBI to routinely search through Americans' communications without a warrant.

The Road Ahead

So where do we go from here? In the last Congress, you proved on a strong bipartisan basis that we do not have to meekly accept this status quo. You demonstrated that it is possible to erect useful guardrails to protect Americans' civil rights against surveillance abuses, 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.

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

- And on the House floor, you came within one 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.

As you do so, moreover, you can rest assured that the American people are behind you. For example, a YouGov poll shows that 76 percent of Americans support a warrant requirement for government inspection of Americans' international communications. As the debate on the reauthorization of Section 702 begins, you can speak and act with confidence, knowing that your constituents are strongly on your side.

Resisting Intelligence Community Misinformation

That is not to say the road will be easy. Last Congress, reform proponents lost the warrant votes because the Intelligence Community (IC) whispered to Members that they would be held responsible for a parade of horribles if those measures passed. That was and is nonsense. You took great care to make sure the intelligence community would retain the authorities it needs to track and counter dangers from here and abroad.

Indeed, the Intelligence Community's own testimony offered only a few scenarios in which U.S. person queries—the warrantless searching of Americans' communications in the Section 702 database—had any value in significant cases. And your proposed warrant rule included reasonable exceptions that allow the government to act effectively in every exceptional circumstance. Let me detail some of the whisperings of the Intelligence Community and the sound policy responses this Committee included in your proposed warrant requirements.

- For example, the IC whispered to Members that a warrant requirement for Section 702 would leave the country wide open to cyberattacks. But your proposed warrant requirement made it clear: Queries focused on cyberthreat signatures were explicitly exempt and usually involve metadata queries, not content. Otherwise, any U.S. company or critical infrastructure target can simply consent to a query.

- The IC also whispered that a warrant requirement for Section 702 would curb the ability to foil foreign plots. You had an answer: Any American targeted for assassination or kidnapping in a foreign plot will obviously give grateful consent for a query designed to protect them.

- The IC further asserted that a warrant requirement would expose us to foreign spying. Your answer was that, because metadata queries are exempt, a warrant rule would not inhibit the government's ability to identify contacts. The government *has never shown one instance* in which queries of actual message *content*—as opposed to identifying metadata—were critical to an investigation of a foreign agent. Besides, isn't reading the private communications of American citizens exactly why the Constitution mandates a warrant?

- Then there was the IC's trump card: What about the scenario of a ticking time bomb? This is perhaps their most hackneyed charge—that we risk lives by allowing for due process and court approval. The fact is that, if such a time-sensitive emergency ever did occur, your warrant rule explicitly accounted for it by including an exception precisely for such exigent circumstances.

- Finally, the IC alleged that a warrant requirement would require an army of additional FBI attorneys and FISA judges. But such a phantom army would never be needed. Attached is an analysis the Project for Privacy and Surveillance Accountability developed together with the Center for Democracy and Technology. In it, we show that the Bureau would at most have to deal with an average of three queries per day requiring a warrant. That may require a very

modest increase in agency and judicial resources, but it's a small price to pay for ensuring Americans' privacy—and compliance with the Fourth Amendment.

The excessive numbers are, in fact, on the other side of the ledger. The Privacy and Civil Liberties Oversight Board (PCLOB) reports that the government has given "little justification" for the value of almost 5 million U.S. person queries conducted from 2019 to 2022. The government could report only a handful of instances in which these searches were useful. And in each of those cases, the government could have easily obtained a warrant or invoked one of your proposed exceptions.

Conclusion

In the face of this well-organized campaign against reform, this Committee has advanced and can continue to advance sensible bipartisan, well-reasoned and thoughtful reforms. In the face of a surveillance state growing at breakneck speed, this Committee has shown leadership and a sense of urgency that matches the moment. We don't have to supinely accept the erosion of all privacy. We don't have to trust that government agents and future administrations will always use these awesome powers solely for national security. These technologies simply offer too much power to trust that future guardians will not be tempted to misuse them, as they have done in the past.

In short, you have shown that you can protect both the constitutional rights of your constituents and also keep them safe from foreign and domestic threats. I urge you to uphold the Constitution by once again advancing—and persuading your fellow Members to adopt—a warrant requirement for both government-purchased data and data collected under Section 702.

Thank you for the opportunity to testify.

Gene Schaerr

PPSA
PROJECT FOR PRIVACY & SURVEILLANCE ACCOUNTABILITY

CENTER FOR DEMOCRACY & TECHNOLOGY

Debunking Myths on the National Security Impact of Warrants for U.S. Person Queries

Warrantless queries of Americans' communications obtained via Section 702 of the Foreign Intelligence Surveillance Act ("FISA 702") are antagonistic to the basic principle of the Fourth Amendment. Deliberately seeking to read Americans' private communications – but without ever showing evidence of wrongdoing or obtaining independent approval from a judge – violates the Constitution, disrespects American values, and opens the door to abuse.

Opponents of FISA reform nonetheless oppose requiring a warrant for U.S. person queries by claiming these queries provide huge value that would be disrupted by a warrant requirement. ***These claims are false – in reality a warrant rule has been carefully designed to account for the limited value that such queries provide.***

MYTH #1: ***U.S. person queries are immensely important in a broad array of situations, making it dangerous to place restrictions on this important tool.***

> **REALITY: Queries only provide value in a limited set of situations, and the warrant rule proposed in 2024 during the 119th Congress provides exceptions to account for all of them.**

Opponents of reform frame U.S. person queries as frequently valuable across a wide set of national security goals and investigations, but the 2023-2024 debate over FISA 702 proved this was false: The Intelligence Community testimony, the President's Intelligence Advisory Board, and the Privacy and Civil Liberties Oversight Board (PCLOB) uncovered only a few distinct scenarios in which U.S. person queries provided value.[1] And the proposed warrant rule includes exceptions that account for all of them.

Under the 2024 proposal, a warrant would not be required 1) when there is consent, 2) to track malware, or 3) for metadata queries:

- *Cyber Attacks*: Queries were most useful in the cybersecurity context, helping the government detect warning signs of future attacks and trace attacks back to their sources. But queries focused on cyberthreat signatures are explicitly exempt. Much of the cybersecurity value of queries focused on network traffic patterns; this involves metadata rather than content, and metadata queries are also exempt from the warrant rule. Most importantly, any U.S. company or critical infrastructure entity targeted for a cyberattack can simply consent to a query.

[1] For additional details, see The Government's Objections to FISA 702 Reform Are Paper Thin | Lawfare; see also Unpacking the President's Intelligence Advisory Board FISA 702 Report | Lawfare.

- *Foreign Plots*: Queries were also described as useful in detecting and responding to foreign assassination and kidnapping plots. But once again, the consent exception directly accounts for this need. A targeted American will obviously gratefully accept such a query to enable government protection.[2]
- *Foreign Recruitment*: Defenders of the status quo cited limited cases in which queries helped the government discover suspicious foreign contacts, assisting the government in investigating whether the U.S. person was a foreign target or foreign agent. But because metadata queries are exempt, a warrant rule would not inhibit the government's ability to identify these contacts. The government *has never shown one instance* in which content queries were critical to advancing an investigation against a foreign agent.[3] Besides, reading the private emails of an American being criminally investigated is exactly what warrants are required for.

MYTH #2: *U.S. person queries need to be done quickly and efficiently, and a warrant rule would slow the process down in a manner that endangers Americans' lives.*

> **REALITY: The government has never shown queries provide time-sensitive responses, and the warrant rule's exceptions account for such a scenario if it ever did emerge.**

A common argument against surveillance reform is the "ticking time bomb" hypothetical in which there simply isn't time to abide by due process and obtain court approval. But the government has never shown a situation in which query results were needed so quickly that obtaining a warrant would be infeasible.[4]

- If a time-sensitive emergency ever did occur, the warrant rule explicitly accounts for it by including an exception for exigent circumstances. Contrary to this complaint's framing, the government has indicated that query results are used primarily during the *early* stages of investigations, or with queries run on targeted victims--in which cases the consent exception makes a warrant unnecessary.

---

[2] In addition to the consent exception addressing this issue, the warrant rule can be satisfied by a probable cause showing that the query *would produce evidence of a crime*; so long as that standard is satisfied it is not necessary to prove that the query subject is a suspected criminal or foreign agent. Therefore, so long as the government can demonstrate probable cause that a query focused on the target of a foreign plot will uncover details of that plot, such a query would receive necessary judicial sign off. The government has regularly obtained warrants for digital searches focused on victims, and there is no reason to expect they could not do so in the context of queries as well. For more information, see Issue Brief: A Warrant Rule for US Person Queries Would Not Prevent Victim-Focused Queries | CDT.

[3] Notably the two independent reviews of FISA 702 only cite *one instance* when a queried individual was later discovered to be a nefarious actor, and this discovery was the product of an "independent investigation" for which the government successfully obtained a warrant. See PIAB FISA 702 Report, p. 36; see also, PCLOB FISA 702 Report.

[4] Intelligence officials sometimes reference the significant length of FISA Title I warrant applications and time spent developing them as the basis to claim that US person query warrants would be equally slow and onerous. But this is not an apt comparison because the warrant proposal allows the government to conduct queries by obtaining either a standard Title III criminal wiretap order *or* a FISA Title I warrant.

In short, the exigent circumstances, consent and metadata exceptions to the proposed warrant requirement almost certainly address and legitimate concerns about the government's ability to respond to threats quickly.

MYTH #3: *Warrants are not feasible given the scale of U.S. person queries conducted; adding this rule would overwhelm intelligence agencies and the courts.*

> **REALITY: By permitting warrantless metadata queries, the warrant rule ensures the government will not need to go to court frequently.**

In 2023, the most recent year for which data is available, the FBI conducted queries for over 57,000 unique U.S. person terms, reflecting unacceptable government overreach and fishing efforts. However, most of these queries do not produce responsive results. Because the proposed warrant requirement would apply only when the government sought to access a communication's content, it would weed out impropriety without straining intelligence agencies or the courts.

- Only 1.58 percent of the FBI's U.S. person queries resulted in personnel accessing content, according to the FBI.[5] Thus, even if queries continued to be conducted at the prior rate of 57,000 annually – an unlikely prospect, given that many of these queries were improper or broad fishing efforts – a warrant would be potentially applicable to less than 1,000 queries a year, less than 3 per day on average. And because the proposed warrant rule would permit warrantless metadata queries (and only require court approval to *access content*), agencies would be able to confirm when a query will yield a "hit" before devoting any time and effort to seeking a warrant.

And even as to these 2-3 queries per day, most would fall under one of the exceptions to the warrant requirement described above. The FBI usually wouldn't need 2-3 warrants each day; more likely it would need to obtain consent of 2-3 entities to help prevent a future cyberattack or foreign plot. And if adding a warrant requirement on this limited level would be too onerous for intelligence agencies or the courts, the solution would be to add personnel to cover that need, not to reject an important constitutional safeguard against abuse.

Americans' basic rights should not be secondary to bureaucratic hurdles and staffing limits. The exceptions and exemptions built into the 2024 warrant proposal would allow the government to remain within the boundaries of the Constitution while also having the means to protect national security.

For additional information, please contact Gene Schaerr (gschaerr@schaerr-jaffe.com), General Counsel at the Project on Privacy and Surveillance Accountability, and Jake Laperruque (jlaperruque@cdt.org), Deputy Director of the Security and Surveillance Project at the Center for Democracy & Technology.

[5] See PCLOB FISA 702 Report, fn. 35.