Statement of Gene Schaerr
General Counsel of PPSA and Managing Partner, Schaerr|Jaffe LLP,
Before the House Subcommittee on Crime and Federal Government Surveillance
July 14, 2023

Dear Chair Biggs, Ranking Member Jackson Lee, and Members of the Subcommittee. Thank you for the opportunity to submit this testimony.

The group of which I am general counsel—the Project for Privacy and Surveillance Accountability, or PPSA—is a civil liberties organization that works closely with groups across the ideological spectrum to address surveillance abuse and the government's encroachments on the Fourth Amendment. Separately, I also represent Carter Page in his lawsuit against those who surveilled him in 2016, although I am not appearing today on his behalf.

Given the perspectives provided by both of those roles, we believe the impending expiration of FISA Section 702 presents a once-in-a-generation opportunity, not only to deal with the specific issues raised by the Carter Page fiasco, but more generally, for Congress to reassert its rightful, constitutional role in determining when, why and how Americans of all political stripes can be subject to surveillance by their own government. Revulsion at unwarranted 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. And today, based on a host of discussions with many civil liberties and other advocacy groups, I'm confident you will find wide support across the ideological spectrum for a broad surveillance reform bill that goes well beyond Section 702.

As evidence of that, as you will see in the appended joint statement, PPSA has joined with other civil liberties groups—from the right, left, and center—in urging Congress to implement in any reauthorization bill five specific principles. Today I will focus on three of those, and how they either apply to or are illustrated by the Carter Page history as well as documented surveillance of people and organizations on the other side of the spectrum.

1. **Any surveillance that impacts Americans should be undertaken *only* pursuant to a statute, duly enacted by the people's representatives in Congress**.

The first principle follows from the "consent-of-the-governed" concept articulated in the Declaration of Independence and embodied in Article I of the Constitution. It is 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 the FBI or any other executive official, none of whom has authority to consent to surveillance on their behalf.

How does that principle apply to FISA reform? Many provisions of FISA have been rendered anachronistic by globalized communications and other technology that has

opened gaps in the law's coverage, allowing the government to collect vast amounts of Americans' communications and other personal data with no statutory limits and no effective congressional oversight. These gaps are exacerbated by Executive Order 12333, which is not a law but is treated by the intelligence community as if it were sacred writ.

The resulting gaps give federal agencies room to conduct sweeping surveillance overseas and to collect geolocation data and other sensitive information inside the United States, subject only to Executive Order 12333 and related agency policies — which include even fewer protections for Americans' rights than Section 702. We now know, for example, that for years—under administrations of both parties—the CIA has exploited these gaps in FISA's reach to conduct a bulk collection program that swept up Americans' sensitive data. Under administrations of both parties, the FBI has routinely conducted "back-door" searches of information collected under Section 702. And of course, the government routinely searches vast additional quantities of Americans' most sensitive information purchased from data brokers. Congress should seize this unique opportunity to bring all of these surveillance methods within a statutory framework that includes adequate guardrails and effective oversight by Congress and the courts.

The now-infamous surveillance of Carter Page itself illustrates the value of such a framework for people of all political affiliations. As you know, Mr. Page was surveilled pursuant to a statute, Title I of FISA, that requires some documentation of who authorized the surveillance, the scope of the surveillance, and the reasons for it. And this documentation helped ensure that the FBI's shenanigans would *eventually* be discovered. Yes, it took far too long, but at least the truth ultimately emerged.

But imagine what would have happened if Mr. Page had been surveilled—as many others on both the right and left have been—under an authority like Section 702 that has no specific judicial oversight. We likely never would have learned of the FBI's abuses, just as we would have remained in the dark if the FBI had surveilled Page pursuant to 12333 or some other claim of executive authority. FISA's legislative framework, although deeply imperfect, at least enabled Congress to uncover the FBI's abuses in the Page case. And that's a powerful reason to bring all other forms of government surveillance of Americans within an appropriate statutory framework.

2. **Any government access to Americans' communications or other private data should be undertaken *only* pursuant to a probable cause judicial warrant**.

The Carter Page saga is also relevant to the second principle that virtually every civil-liberties group in the country is urging Congress to adopt as a condition of reauthorizing Section 702—that any government access to Americans' communications or other private data be allowed *only* pursuant to a judicial order, issued under the Fourth Amendment's probable cause standard. As we saw in the Page case, the existence of such a requirement under Title I helped create a paper trail that, in turn, ultimately revealed the FBI's wrongdoing.

But beyond the deterrence provided by such paper trail, as the framers of the Fourth Amendment recognized, a warrant requirement is important because it helps prevent 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 the massive trove of information compiled under Section 702.

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, surveillance under Section 702 inevitably sweeps up vast amounts of *Americans'* communications.

As the FBI admitted just the other day, moreover, it sometimes conducts "backdoor searches" of those communications and other data in ordinary domestic criminal cases, and believes it has the right to do so routinely. And, after years of insisting it could not provide this information, it was reported that the FBI had performed 3.4 million backdoor searches in 2021 alone. Yes, the FBI now claims that refinements in its internal procedures have dramatically reduced these numbers to 204,000 queries of 119,383 individuals. Under any accounting, that would still amount to massive violations of Americans' privacy. There is little reason to believe the FBI would not again revert to conducting millions of backdoor searches if strong legislative reforms are not enacted.

Further, according to several recent FISA Court opinions, the FBI routinely conducts those backdoor searches in politically sensitive cases. For example, in violation of its own rules, 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 apply 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.

Worse, what the FBI and other government agencies don't extract directly from Section 702 surveillance they can now simply purchase from data brokers. Americans' sensitive personal communications and data—including highly personal geolocation data and other Fourth Amendment-protected information—are routinely scraped from apps and sold by third-party data brokers to government law enforcement and intelligence agencies. This is done without any statutory guardrails or judicial oversight. As a result, agency lawyers maintain they can review Americans' personal information simply by reaching into the federal wallet—no statutory authorization needed.

Congress should put a stop to the government's use of Section 702 and other surveillance authorities and mechanisms as end-runs around Americans' Fourth

Amendment rights. And it should do so by imposing a probable-cause warrant requirement on all direct *and indirect* searches of Americans' private data by federal agencies.

3. **Any surveillance that impacts Americans should be subject to adequate mechanisms—in both Congress and the judiciary—to ensure accountability for compliance with governing law**.

Even with statutory guardrails, and even with a probable-cause requirement, egregious violations of Americans' privacy can still occur absent adequate accountability. Whatever our political leanings, we should all be concerned that an investigation by the Department of Justice's own Inspector General, Michael Horowitz, found that the FBI's four applications to surveil Mr. Page—then an aide to a major presidential candidate—were rife with errors of omission and commission. Later, an FBI attorney was convicted of falsifying a document submitted in that case.

The Page incident, moreover, inspired Mr. Horowitz to test a sample of 29 other FISA applications. And in that sample alone, Horowitz's team found "over 400 instances of non-compliance with the Woods Procedures"—procedures designed to ensure the accuracy of submissions in *ex parte* FISA Court hearings in which only the government is present.

That's why the upcoming revamp of FISA must go well beyond ensuring that Congress itself has the tools to conduct necessary oversight of surveillance agencies—including sufficiently cleared staff for each Member. That revamp must also include measures like enhanced penalties for violating statutory guardrails, for lying to courts, and for refusing to comply with statutory reporting requirements. There should be meaningful consequences for violating the Constitution and other duly enacted laws.

One particularly useful oversight mechanism would be an enhanced system of "amici" or "friends of the court," who can participate in proceedings before the FISA Court in a wide range of sensitive investigative matters. A bipartisan amendment to that effect by Senators Lee and Leahy passed the Senate by an overwhelming margin—77 to 19—in 2020.

If such an amicus had been appointed in the Carter Page case, it's very unlikely he would have been subjected to surveillance at the hands of the FBI. First, if the FBI personnel drafting and signing the applications had known they would be reviewed by an amicus charged with protecting Americans' privacy, those personnel likely would not have risked lying and fabricating evidence—for fear of being caught and punished by the court. And second, if such misconduct *did* occur, the presence of an amicus would at least make it more likely that it would be caught before the warrant issued, and correspondingly less likely that another citizen's privacy would be egregiously violated. So something like the Lee-Leahy amendment should be part of any Section 702 reauthorization package, and it should apply to any sensitive investigation of people on the political right, left, or center.

Conclusion

By adhering to the five principles proposed by our bipartisan, pan-ideological coalition, you, as the People's agents, can end what has unfortunately become a game of surveillance whack-a-mole. You can—and we believe you must—assert your constitutional authority against an executive branch that, regardless of the party that controls it, is too often overbearing. And you can and must assert your authority against a judicial branch that too often gives the executive an undeserved benefit of the doubt. Please don't let this once-in-a-generation opportunity slip away.

ACLU • Americans for Prosperity • Brennan Center for Justice • Demand Progress Action • Due Process Institute • Electronic Privacy Information Center • FreedomWorks • Project for Privacy & Surveillance Accountability • Restore the Fourth • Wikimedia Foundation

Congress Should Not Reauthorize FISA Section 702 Without Satisfying Key Protections for Americans' Civil Liberties

By the end of 2023, Congress must decide whether to reauthorize Section 702 of the Foreign Intelligence Surveillance Act. Section 702 was intended to provide U.S. agencies with the statutory authority to collect intelligence only from foreigners abroad. Unfortunately, for over a decade, agencies have abused this authority, using loopholes in Section 702 to conduct warrantless surveillance on millions of Americans.

For example, a report published by ODNI in April 2022 disclosed that, in 2021 alone,

the FBI conducted as many as 3.4 million searches of Section 702-acquired data for information about *Americans* and their communications. And in 2018, Foreign Intelligence Surveillance Court (FISC) Judge James Boasberg rebuked the FBI for improper use of 702 databases against Americans. The misuse of this surveillance is "widespread." The FISC also revealed that the FBI has used warrantless NSA data in a range of cases involving purely domestic issues.

Such a system is worse than broken. It is assembling the elements for a pervasive, unaccountable surveillance state. Congress should not reauthorize Section 702 without making significant reforms to ensure these abuses do not continue under any authority.

Legislation that reauthorizes Section 702 must ensure compliance with key principles:

1. **Any surveillance that impacts Americans should be undertaken *only* pursuant to a statute, duly enacted by the people's representatives in Congress**.
2. **Any government access to Americans' communications or other Fourth Amendment-protected data should be undertaken *only* pursuant to a probable cause judicial warrant**.
3. **Any surveillance that impacts Americans should be subject to adequate mechanisms—in both Congress and the judiciary—to ensure accountability for compliance with governing law**.
4. **The government should not be able to buy its way around legal limits on collecting and accessing Americans' information**.
5. **Surveillance should be no broader than necessary to protect our security**.

These principles are critical to Americans' privacy and civil liberties. In 2023, Congress must end the pervasive abuse of Section 702 and other surveillance authorities.