No. 22-190

In the Supreme Court of the United States

WIKIMEDIA FOUNDATION,
Petitioner,

v.

NATIONAL SECURITY AGENCY/
CENTRAL SECURITY SERVICE, *et al.*,
Respondents.

On Petition for a Writ of Certiorari to the
United States Court of Appeals for the Fourth Circuit

BRIEF OF THE BRENNAN CENTER FOR JUSTICE, CLAUSE 40 FOUNDATION, DUE PROCESS INSTITUTE, ELECTRONIC FRONTIER FOUNDATION, ELECTRONIC PRIVACY INFORMATION CENTER, FREEDOMWORKS FOUNDATION, PROJECT FOR PRIVACY AND SURVEILLANCE ACCOUNTABILITY, AND TECHFREEDOM AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

CHRIS SWIFT
Davis Wright Tremaine LLP
1300 SW Fifth Avenue
Suite 2400
Portland, OR 97201

ELIZABETH GOITEIN
Brennan Center for Justice
at NYU School of Law
1140 Connecticut Ave. NW
Suite 1150
Washington, DC 20036

DAVID M. GOSSETT
Counsel of Record
MEENAKSHI KRISHNAN
Davis Wright Tremaine LLP
1301 K Street NW
Suite 500 East
Washington, DC 20005
(202) 973-4200
davidgossett@dwt.com

Counsel for Amici Curiae

LEGAL PRINTERS LLC ● Washington, DC ● 202-747-2400 ● legalprinters.com

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

FEDERAL CASES

FISC CASES

FEDERAL STATUTES

RULES

OTHER AUTHORITIES

INTERESTS OF *AMICI CURIAE*

This brief is submitted jointly by the Brennan Center for Justice, Clause 40 Foundation, Due Process Institute, Electronic Frontier Foundation, Electronic Privacy Information Center, FreedomWorks Foundation, the Project for Privacy and Surveillance Accountability, and TechFreedom as *amici curiae* in support of Petitioner.[1]

The Brennan Center for Justice at NYU School of Law is a non-partisan public policy and law institute focused on fundamental issues of democracy and justice.[2] The Center's Liberty and National Security Program uses innovative policy recommendations, litigation, and public advocacy to advance effective national security policies that respect the rule of law and constitutional values. One of the Program's main areas of research and advocacy is foreign intelligence surveillance. Program staff have produced in-depth research reports on the topic; submitted *amicus* briefs in connection with FISA litigation; published op-eds and blog posts; and testified before the Senate and House Judiciary Committees regarding FISA on multiple occasions.

Due Process Institute and its sister organization, Clause 40 Foundation, are nonprofit, bipartisan,

---

[1] Counsel of record for all parties received notice of *amici*'s intent to file this brief at least 10 days before the due date, and all parties consented to its filing. Pursuant to Rule 37.6, no counsel for a party authored this brief in whole or in part, and no person or entity other than *amici* and their counsel made a monetary contribution intended to fund the preparation or submission of this brief.

[2] *Amicus* does not purport to represent the position of the NYU School of Law.

public interest organizations that work to honor, preserve, and promote the constitutionally guaranteed due process rights in the criminal legal system. This case is of significant concern to these organizations because of the fundamental importance of protecting the people against unconstitutional governmental overreach via the use or abuse of its foreign intelligence surveillance authorities.

The Electronic Frontier Foundation (EFF) works to protect civil liberties and preserve privacy rights in the digital world, supported by more than 38,000 dues-paying members. EFF has litigated issues involving FISA and the state-secrets privilege. It has a strong interest in ensuring that civil litigation challenges to the lawfulness of government surveillance programs can proceed as Congress intended. It has an equally strong interest in ensuring the state-secrets privilege remains within the limits established by the Court and is not expanded to shield government abuses and illegal conduct from judicial scrutiny. EFF has served as counsel in lawsuits with FISA and state-secrets issues, and has served as amicus on state-secrets cases in this Court.

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC has fought for public access to records about the government's assertion of surveillance authority. EPIC has also brought challenges to the NSA telephone record collection program in this Court and has appeared as *amicus* in cases concerning the ability of individuals to challenge national security surveillance.

FreedomWorks Foundation is a nonprofit, nonpartisan grassroots organization dedicated to upholding free markets and constitutionally limited government. Founded in 2004, FreedomWorks Foundation is among the largest and most active right-leaning grassroots organizations, amplifying the voices of millions of activists both online and on the ground. FreedomWorks Foundation has been actively involved in education about the threats to due process, free speech, and dissent posed by warrantless collection of and access to Americans' data and communications by the NSA, and was previously a plaintiff in a civil suit against the NSA mass metadata collection.

The Project for Privacy & Surveillance Accountability (PPSA) is a nonprofit, nonpartisan organization that focuses on a range of privacy and surveillance issues, including by helping private citizens vindicate their rights when the government violates them in the name of national security.

TechFreedom is a nonprofit, nonpartisan think tank dedicated to educating policymakers, the media, and the public about technology policy. TechFreedom defends the freedoms that make technological progress both possible and beneficial, including the civil rights that protect against undue and unjust government surveillance.

INTRODUCTION AND SUMMARY OF ARGUMENT

This Court should grant certiorari to ensure that Petitioner can obtain judicial review through civil litigation of the significant legal questions posed by Foreign Intelligence Surveillance Act (FISA) surveillance. The federal government engages in

surveillance on a far greater scale and with far fewer safeguards than our nation's founders ever could have anticipated. Under Section 702 of FISA, the government searches communications en masse—including those of Americans—as they flow through the Internet backbone. Using this technique, known as "Upstream" surveillance, the government has intercepted billions of communications without any court reviewing or approving the individual targets of the surveillance.

FISA sought to strike a balance by providing for judicial review of foreign intelligence surveillance efforts in three primary ways: Foreign Intelligence Surveillance Court (FISC) proceedings, criminal prosecutions, and civil litigation. But experience has shown that the former two mechanisms neither provide meaningful review nor sufficiently protect constitutional rights. Without this Court's intervention, the lower court's improper application of the state secrets privilege will eviscerate the last remaining option for judicial review of FISA surveillance—civil litigation.

1. This Court should grant certiorari to preserve the civil litigation challenges to FISA surveillance that Congress has expressly authorized. Plaintiffs may seek judicial review of FISA surveillance by bringing a claim for damages under 50 U.S.C. § 1810. This provision evinces Congress's intent that civil litigation serve as a check on FISA abuses. When combined with this Court's recent ruling in *FBI v. Fazaga*, 142 S. Ct. 1051 (2022), the Fourth Circuit's dismissal of a lawsuit based on the state secrets privilege, even though the plaintiff could prove its case without privileged evidence, effectively discards this oversight mechanism. Unless this Court

intervenes, the lower court's decision leaves litigants with no meaningful judicial recourse to challenge FISA surveillance because, as discussed in Parts II and III, FISC proceedings and criminal prosecutions are not adequate alternatives. *See* Part I, *infra*.

2. FISA generally requires FISC authorization before the government conducts foreign intelligence surveillance that targets U.S. persons or takes place inside the United States. 50 U.S.C. § 1805. But this review is largely non-adversarial and ex parte. Judicial review of Section 702 surveillance is even more circumscribed, permitting mass surveillance without any individualized court review or approval of the targets of surveillance. 50 U.S.C. § 1881a. And in both contexts, the government has frequently submitted inaccurate or misleading information. The predictable result has been a failure by the FISC to reliably check unlawful surveillance. *See* Part II, *infra*.

3. Nor are challenges in criminal prosecutions effective. In theory, defendants may challenge evidence obtained through FISA surveillance when the government attempts to use that evidence in a criminal prosecution. 50 U.S.C. § 1806(e). But in practice, the government rarely provides notice to FISA surveillance targets, particularly of Section 702 surveillance. Even when it does, defendants cannot effectively challenge surveillance because they are denied access to the relevant underlying materials. Moreover, the provisions for challenges by criminal defendants apply only where the government initiates a criminal prosecution. Where, as is frequently true with Section 702, the government engages in surveillance but does not prosecute the targets of that surveillance, these provisions have no relevance.

Therefore, criminal prosecutions similarly fail to offer meaningful review of FISA surveillance. *See* Part III, *infra*.

* * * * *

Because of the shortcomings in FISC proceedings and in challenges to FISA evidence in criminal prosecutions, no court in either context is likely ever to fully review the government's Upstream surveillance program. This renders civil litigation the sole bulwark against government overreach, not only with respect to Upstream but likely for FISA activities more generally. But the Fourth Circuit's improper application of the state secrets privilege would effectively eliminate this protection, too. This Court's intervention is therefore necessary to preserve civil litigation as a viable means to challenge FISA surveillance.

ARGUMENT

I. This Court's Intervention Is Necessary To Preserve Civil Litigation Challenges To FISA Surveillance.

Congress established three mechanisms for obtaining judicial review of FISA surveillance: FISC proceedings, challenges in criminal prosecutions, and civil litigation. As we discuss below, however, neither FISC proceedings nor criminal prosecutions have been effective checks on FISA abuses. Intervention by this Court is therefore necessary to ensure that civil litigation remains available to fill the void. Absent this Court's review, the government will be able to rely on the state secrets privilege to circumvent judicial review of FISA surveillance even in cases in which the plaintiff seeks to proceed only on the basis of non-secret evidence. Such an outcome would be

inconsistent with congressional intent and the preservation of constitutional liberties.

FISA's text expressly authorizes judicial review in civil cases in traditional federal courts. Congress provided a cause of action for damages against individuals responsible for FISA violations. *See* 50 U.S.C. § 1810. And it waived sovereign immunity for some FISA violations. *See* 18 U.S.C. § 2712.

The decision below held that the government may obtain dismissal of constitutional claims by asserting that it would need privileged evidence to mount any hypothetical defense. Pet. App. 5a. As Petitioner explains, this decision conflicts with this Court's precedent in *United States v. Reynolds*, 345 U.S. 1 (1953), and *General Dynamics Corp. v. United States*, 563 U.S. 478 (2011), which hold that the privilege is merely an evidentiary one. As with all other evidentiary privileges, the rule is that privileged evidence simply drops out of the case, and the litigation proceeds without it. Accordingly, as long as a plaintiff can make out a *prima facie* case without resort to privileged evidence—as is the case here—the privilege provides no ground for dismissal. Pet. 20-24.

If this Court does not intervene, an invocation of the state secrets privilege may now be used to mandate automatic dismissals in virtually every case involving FISA surveillance. FISA surveillance applications are always classified and will thus automatically trigger a claim of state secrets privilege. Much of the information relating to programmatic surveillance under Section 702 is similarly classified. And it is reasonable to expect that the government will assert a need for this information in defending against claims of unlawful FISA surveillance. The state secrets privilege, as interpreted and applied by

the Fourth Circuit, would thus stymie civil litigation over FISA abuses.

This result is especially likely in light of this Court's ruling in *Fazaga* that Section 1806(f) does not displace the state secrets privilege. 142 S. Ct. at 1060. Section 1806(f) applies in cases involving electronic surveillance. It requires courts, when presented with a government assertion that the disclosure of information through litigation would harm national security, to examine the surveillance materials in camera and ex parte and rule on the lawfulness of surveillance. Under *Fazaga*, the government may bypass this set of procedures by invoking the state secrets privilege. As a practical matter, this means that the legal review contemplated by Section 1806(f) is unlikely to take place in civil litigation.

In light of *Fazaga*, it is all the more important that the state secrets privilege not be construed to close the door to civil lawsuits where plaintiffs can prove their case with non-privileged evidence. Especially given the well-documented limitations of FISC proceedings and challenges to FISA surveillance in criminal prosecutions discussed below, the lower court's erroneous conception of the state secrets privilege would undermine the accountability needed to safeguard Americans' liberty and privacy and leave individuals with little protection against unlawful surveillance. This Court's intervention is the only means of preventing that outcome.

II. FISC Proceedings Do Not Adequately Protect Against Government Abuses.

The Fourth Circuit's decision is particularly problematic given the demonstrated ineffectiveness of

other means to enforce constitutional limits on FISA surveillance.

The government generally must obtain authorization from the FISC before conducting foreign intelligence surveillance of U.S. persons or inside the United States, 50 U.S.C. § 1805, and must obtain FISC approval to conduct programmatic surveillance under Section 702, including Upstream. 50 U.S.C. § 1881a. But FISC oversight has proven insufficient to protect against government overreach.

It "takes little imagination" to appreciate the risks presented by ex parte proceedings. *Kaley v. United States*, 571 U.S. 320, 355 (2014) (Roberts, C.J., dissenting). "[C]ommon sense" dictates that "decisions based on only one side of the story will prove inaccurate more often than those made after hearing from both sides." *Id.* The risks of ex parte proceedings—one-sided, inaccurate factual presentations and distorted legal outcomes—have materialized, time and time again, in FISC proceedings.

A. FISC proceedings lack the adversarial process essential to effective judicial review.

An open, adversarial process is a bedrock of the American judicial system. "[F]airness can rarely be obtained by secret, one-sided determination of facts decisive of rights." *Joint Anti-Fascist Refugee Comm. v. McGrath*, 341 U.S. 123, 170 (1951) (Frankfurter, J., concurring). While adversarial proceedings do not "magically eliminate all error," informed advocacy on both sides of a case "substantially reduce[s] its incidence." *Alderman v. United States*, 394 U.S. 165, 184 (1969). Proceedings before the FISC, however, are ex parte and lack the hallmarks of our adversarial system. And the provisions Congress enacted in 2015

for the use of *amici* were far from sufficient to solve the problems inherent in non-adversarial processes.

Initially, the FISC considered government applications to conduct domestic electronic surveillance of specific individuals for foreign intelligence purposes—a process designed to mirror the issuance of warrants and wiretaps in traditional criminal proceedings, which are conducted ex parte. *See generally* Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, 92 Stat. 1783 (1978).

But, as amendments to FISA expanded the statute, so too did the types of matters the FISC was required to consider ex parte. FISA was amended to encompass a growing body of surveillance techniques, like physical searches, 50 U.S.C. §§ 1821-1829; pen registers/trap and traces, 50 U.S.C. §§ 1841-1846; and the compelled disclosure of certain business records, 50 U.S.C. §§ 1861-1864. For decades, these types of applications, too, were considered ex parte by the FISC.

Beginning in 2004, the FISC's role began to change even more fundamentally. For the first time, the government sought FISC review and approval of increasingly complex *programmatic* surveillance activities. These activities presented sophisticated technical questions, along with complex and novel questions of federal statutory and constitutional law; at times, they encompassed mass surveillance of the communications of millions of Americans. Walter Mondale, et al., *No Longer a Neutral Magistrate: The Foreign Intelligence Surveillance Court in the Wake of the War on Terror*, 100 MINN. L. REV. 2251, 2270-72 (2016). This, too, was *all* done ex parte.

In 2008, Congress enacted Section 702, a law permitting surveillance of foreign targets overseas without any individualized court approval despite the certainty that such surveillance would sweep in the communications of large numbers of Americans. Congress charged the FISC with annually approving the general Section 702 surveillance procedures. This task requires in-depth statutory and constitutional analysis and an accurate understanding of highly complex surveillance practices—again without the benefit of adversarial proceedings.

FISA amendments in 2015 did establish a presumption that FISC judges should appoint *amici* in cases that present "a novel or significant interpretation of the law." 50 U.S.C. § 1803(i)(2)(A). But this *amicus* provision still does not guarantee an adversarial process. Among other problems, the FISC may decline to appoint *amici* if it determines that such appointment is "not appropriate," *id.*; and even when appointed, *amici* are not required to oppose the government's positions, and therefore do not serve as a proxy for an opposing party. *See* 50 U.S.C. § 1803(i)(4); *see also* 166 CONG. REC. S2410-2412 (daily ed. May 13, 2020) (statement of Sen. Leahy) (describing proposed amendments to FISA *amicus* provision).

B. The government has repeatedly provided the FISC with materially incomplete or misleading information.

The FISC's ex parte consideration of increasingly complex surveillance techniques potentially affecting millions of Americans coincided with another troubling development: increasing evidence that the government was presenting false or misleading information to the FISC.

This problem has afflicted all aspects of FISA surveillance. The government has publicly disclosed, for example, that since 2004, it has sought FISC approval for at least three types of programmatic, mass surveillance—domestic internet metadata, domestic phone records, and, under Section 702, international communications. At various points, the government provided incomplete or misleading information to the FISC about *each* of these programs, leading the court to authorize surveillance based on incorrect or incomplete understandings of the programs' operation. Often, the misrepresentations effectively concealed the government's failure to comply with the law or with court-imposed rules.

The first of these programs—mass surveillance of domestic internet metadata—was marked by a "history of material misstatements" about the program and repeated "non-compliance" with FISC orders. *[Redacted]*, No. PR/TT [Redacted], at 72 (FISC [Date Redacted]).[3] For years, the government "exceeded the scope of authorized acquisition continuously," without the court's knowledge. *Id.* at 2-3. These were no mere technical violations: "[V]irtually every" record generated by the metadata program "included some data that had not been authorized for collection." *Id.* at 21.

The government also engaged in "systematic noncompliance" with FISC-mandated procedures while conducting its program of mass surveillance of domestic phone records. *In re Production of Tangible Things from [Redacted]*, No. BR 08-13, at 10 (FISC

[3] *Available at* https://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf.

Mar. 2, 2009).[4] The government "compounded its non-compliance" by "repeatedly submitting inaccurate descriptions" of the program's operation, *id.* at 6, leading the FISC to authorize surveillance "premised on a flawed depiction" of the program. *Id.* at 10-11 (noting the FISC's "misperception" was "buttressed by repeated inaccurate statements made in the government's submissions"). Ultimately, the FISC lost all confidence that "the government [was] doing its utmost to ensure that those responsible for implementation [of the program] fully compl[ied] with the Court's orders." *Id.* at 12. Again, the errors that were withheld from the court were not minor: The FISC observed that the court-approved rules governing the program "have been so frequently and systemically violated that it can fairly be said that this critical element of the overall [phone records] regime has never functioned effectively." *Id.* at 11.

In addition, the government repeatedly provided materially incomplete or misleading information to the FISC about its Section 702 surveillance—including Upstream. In 2011, the court learned, through a belated disclosure by the government, that "the volume and nature of the information [the government was] collecting" through Upstream was "fundamentally different from what the Court had been led to believe." [*Redacted*], No. [Redacted], at 28 (FISC Oct. 3, 2011).[5] This disclosure "fundamentally alter[ed] the Court's understanding of the scope of the collection," *id.* at 15, and it marked "the third instance in less than three years in which the government

---

[4] *Available at* https://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf.

[5] *Available at* https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf.

ha[d] disclosed a substantial misrepresentation regarding the scope of a major collection program." *Id.* at 16 n.14.

Four years later, the government disclosed another significant compliance incident under Section 702 involving the failure to purge improperly collected communications. The FISC wrote: "Perhaps more disturbing and disappointing than the NSA's failure to purge this information for more than four years, was the government's failure to convey to the Court explicitly during that time that the NSA was continuing to retain this information." *[Redacted]*, No. [Redacted] at 58 (FISC Nov. 6, 2015).[6] Another FISC opinion describes violations of the FISC's orders that occurred "with much greater frequency" than the government had previously disclosed, suggesting a "widespread" problem with Section 702 surveillance. *[Redacted]*, No. [Redacted] at 19 (FISC Apr. 26, 2017).[7] Yet another FISC opinion described "documented misunderstandings" of relevant FISC-imposed standards that led to "broad and apparently suspicionless" queries of communications obtained through Section 702 and lengthy government "delays in reporting" violations to the FISC. *[Redacted]*, No. [Redacted] at 76-77, 82 (FISC Oct. 18, 2018).[8] And in 2021, the government released a FISC opinion involving Section 702 in which the court recounted a "particularly concerning" "system failure" that

---

[6] *Available at* https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.

[7] *Available at* https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf.

[8] *Available at* https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf.

resulted in noncompliance with a court-imposed documentation requirement, which went "undetected or unreported for nearly a year." FISC *[Redacted]*, No. [Redacted] at 50-51 (FISC Nov. 18, 2020).[9]

The government's misrepresentations to the FISC are not limited to the operation of its mass surveillance programs; all types of proceedings before the FISC appear to be infected with inaccuracies and errors. In December 2019, a report from the Department of Justice Inspector General reviewed four FISA applications submitted as part of the FBI's investigation into alleged Russian interference in the 2016 presidential election. *See* Dep't of Justice, Office of Inspector General, *Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation* (Dec. 2019).[10] The report identified 17 separate problems with the FBI's applications to the FISC, representing "serious performance failures by the supervisory and non-supervisory agents with responsibility over the FISA applications." *Id.* at viii-xiii. These errors "raised significant questions regarding the FBI chain of command's management and supervision of the FISA process." *Id.* at xiv.

The IG's report led the FISC to question the reliability of FBI information in other FISA applications. *See In re Accuracy Concerns Regarding FBI Matters Submitted to the FISC,* No. Misc. 19-02,

---

[9] *Available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_FISC%20Cert%20Opinion_10.19.2020.pdf.

[10] *Available at* https://www.justice.gov/storage/120919-examination.pdf.

at 2-3 (FISC Dec. 17, 2019).[11] The FISC noted that the "frequency with which representations made by FBI personnel turned out to be unsupported or contradicted by information in their possession, and with which they withheld information detrimental to their case, calls into question whether information contained in other FBI applications is reliable." *Id.* at 3; *see also In re Accuracy Concerns Regarding FBI Matters Submitted to the FISC*, No. Misc. 19-02, at 1 (FISC Mar. 4, 2020).[12]

The IG thus expanded his inquiry, reviewing "a judgmentally selected sample of 29 [FISA] applications relating to U.S. Persons and involving both counterintelligence and counterterrorism investigations" to assess the FBI's compliance with the "Woods Procedures"—the FBI's procedures to ensure the accuracy of facts submitted in FISC surveillance applications. *See* Dep't of Justice, Office of Inspector General, *Management Advisory Memorandum for the Director of the FBI Regarding the Execution of Woods Procedures for Applications Filed with the FISC Relating to U.S. Persons*, at 2 (Mar. 2020).[13] The IG's initial report concluded that 25 of the 29 applications contained "apparent errors or inadequately supported facts." *Id.* at 3. For four FISA applications, the FBI could not locate the files containing the requisite documentation. *Id.* at 2-3. And for three of those four missing files, the FBI "did

---

[11] *Available at* https://www.fisc.uscourts.gov/sites/default/files/MIsc%2019%2002%20191217.pdf.

[12] *Available at* https://www.fisc.uscourts.gov/sites/default/files/Misc%2019%2002%20Opinion%20and%20Order%20PJ%20JEB%20200304.pdf.

[13] *Available at* https://oig.justice.gov/sites/default/files/reports/a20047.pdf.

not know if [the requisite documentation] ever existed." *Id.* at 3. The IG's report provided the FISC, yet again, with "further reason for systemic concern." *In re Accuracy Concerns Regarding FBI Matters Submitted to the FISC,* No. Misc. 19-02, at 2-3 (FISC Apr. 3, 2020).[14]

Following a closer look at the 29 FISA applications, the IG issued a final report in September 2021. *See* Dep't of Justice, Office of Inspector General, *Audit of the Federal Bureau of Investigation's Execution of Its Woods Procedures for Applications Filed with the Foreign Intelligence Surveillance Court Relating to U.S. Persons* (Sept. 2021).[15] It revealed "over 400 instances of non-compliance with the Woods Procedures." *Id.* at 7. The IG also reviewed the results of an FBI inventory of Woods files for approximately 7,000 FISA applications for the period 2015-2020. The Woods files were incomplete or non-existent in 183 cases. *Id.* at 8.

Unsurprisingly, the FISC has described the government's interactions with the court as being marked by an "institutional 'lack of candor.'" *[Redacted]*, No. [Redacted], at 19 (FISC Apr. 26, 2017).[16] Indeed, the FISC has observed that the government "has exhibited a chronic tendency" to provide inaccurate, incomplete, or materially misleading information to the FISC in its filings.

---

[14] *Available at* https://www.fisc.uscourts.gov/sites/default/files/Misc%2019%2002%20Order%20PJ%20JEB%20200403.pdf.

[15] *Available at* https://oig.justice.gov/sites/default/files/reports/21-129.pdf.

[16] *Available at* https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf.

[Redacted], No. [Redacted], at 13-14 (FISC [Date Redacted]).[17]

C. The lack of an adversarial process and the government's "lack of candor" render the FISC's review process unreliable.

As discussed, FISC proceedings generally involve only one party, and that party exhibits "a chronic tendency" to provide misleading information. It should come as no surprise that this process does not consistently yield fair and reliable outcomes.

The FISC's consideration of the NSA's program of mass surveillance of domestic call records illustrates the problem. That program—under which the NSA collected billions of records about Americans' phone calls—ostensibly operated under Section 215 of the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001), which amended FISA's business records provision.[18] Section 215 authorized ex parte applications to the FISC to compel the production of specific "tangible things," such as business records or documents, if the government could show they were relevant to an authorized counterterrorism, counter-espionage, or foreign intelligence investigation.

Even though this statutory authority was explicitly no broader than a grand jury or similar subpoena authority, 50 U.S.C. § 1861(c)(2)(D), the government interpreted it to allow the compelled disclosure of billions of records of calls made to and from Americans.

---

[17] *Available at* https://www.documentcloud.org/documents/4780432-EFF-Document-2.html.

[18] 50 U.S.C. § 1861 (2012). Section 215 expired in 2020 when Congress failed to pass reauthorizing legislation.

The FISC's initial order authorizing the mass collection of Americans' call records under Section 215—an order unprecedented in the history of American surveillance—was a brief and largely perfunctory recitation of the statutory requirements for issuance of an order. *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 06-05 (FISC May 24, 2006).[19] At the time, the government failed to bring to the court's attention another statute, the Stored Communications Act, 18 U.S.C. § 2701, et seq. (SCA), specifically governing the disclosure of call records from telecommunications providers. Although the SCA was plainly necessary to the FISC's consideration of the program from the outset, the FISC did not consider that statute until nearly two years after the program began. *See In re Production of Tangible Things from [Redacted],* No. BR 08-13 (FISC Dec. 12, 2008).[20]

In fact, the FISC did not fully review the program's constitutional or statutory basis in a written opinion until 2013—*seven years* after the FISC's first authorization of the program. *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted],* No. BR 13-109, 2013 WL 5741573 (FISC Aug. 29, 2013). Not coincidentally, this review occurred shortly after the secrecy of the program was pierced by Edward Snowden's disclosures. And, although this post hoc ex parte review upheld the NSA program, *id.,* two years

---

[19] *Available at* https://www.dni.gov/files/documents/section/pub_May%2024%202006%20Order%20from%20FISC.pdf.

[20] *Available at* https://www.dni.gov/files/documents/section/pub_Dec%2012%202008%20Supplemental%20Opinions%20from%20the%20FISC.pdf.

later—after public, adversarial testing of the substantive legal basis for the phone records program—two different federal courts concluded that the program was illegal. *See ACLU v. Clapper,* 785 F.3d 787 (2d Cir. 2015); *Klayman v. Obama,* 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated on standing grounds,* 800 F.3d 559 (D.C. Cir. 2015). A third federal court reached the same conclusion in 2020. *United States v. Moalin*, 973 F.3d 977 (9th Cir. 2020).

Lacking an adversarial process to air all of the legal arguments against the program and to force the FISC to grapple with those arguments, the FISC allowed the government to collect billions of call records under a mass surveillance program of at best dubious legality—and one whose actual operation often differed significantly from the government's portrayals.

The same conditions that led to a flawed outcome in that instance—secret, one-sided proceedings combined with an "institutional lack of candor" on the part of the government—are all the more pronounced in the FISC's review of Section 702. Even compared with other FISA provisions, the FISC's review of Section 702 is more "narrowly circumscribed." *In re Proceedings Required by § 702(i) of FISA Amendments Act*, Misc. No. 08-01, 2008 WL 9487946, at *2 (FISC Aug. 27, 2008).

Indeed, there is no better illustration of the limits of the FISC's review than Upstream surveillance. Upstream comprises a relatively small percentage of the surveillance the government conducts under Section 702, [*Redacted*], No. [Redacted], at 29-30

(FISC Oct. 3, 2011),[21] but it poses particularly acute constitutional concerns in light of its dragnet scanning of communications traversing the Internet backbone. And yet, despite annually reviewing and approving Section 702 surveillance for more than a decade, the FISC has never addressed the constitutional challenges to Upstream surveillance that Petitioner raises here.

III. FISA Challenges In Criminal Prosecutions Also Do Not Adequately Protect Against Government Abuses.

Nor have criminal prosecutions proven to be an adequate substitute for the type of civil litigation that Petitioner sought to bring here. In criminal prosecutions, initial ex parte warrant proceedings are tolerated because later safeguards exist: Once the government brings charges, searches can be challenged; facts can be contested; affiants can be impeached. But adversarial testing of FISA surveillance in criminal proceedings has proven a poor mechanism for challenging unlawful surveillance.

One serious impediment to such challenges is the government's avoidance of FISA's requirement that notice be provided when the government intends to use evidence "obtained or derived from" FISA surveillance against an "aggrieved person." 50 U.S.C. § 1806(c). This requirement permits the aggrieved person to then move to suppress evidence obtained through unauthorized surveillance. *Id.* § 1806(e).

Notice that Section 702 surveillance will be used in a criminal prosecution is exceedingly rare. In the

---

[21] *Available at* https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf.

first five years the government conducted Section 702 surveillance, it provided notice to *zero* defendants—even as the government intercepted billions of communications during that same period. This stemmed from the government's adoption of an unjustifiably narrow interpretation of its FISA disclosure obligations, and the resulting practice—known as "parallel construction"—of masking evidentiary trails that would have required notice to criminal defendants and allowed FISA surveillance to be challenged. *See* Mondale, *No Longer a Neutral Magistrate*, 100 MINN. L. REV. at 2283.[22]

Eventually, the government notified a handful of defendants whose prosecutions involved evidence derived from Section 702 surveillance—often belatedly and sometimes even after sentencing. *See United States v. Muhtorov,* 187 F. Supp. 3d 1240, 1242 (D. Colo. 2015) ("[B]elated notice in this case was part of the Snowden fallout and the revelation, post-*Clapper,* that the Executive Branch does, in fact, use FAA-acquired information to investigate U.S. persons for suspected criminal activity[.]"), *aff'd*, 20 F.4th 558

---

[22] In *Clapper v. Amnesty International USA,* 568 U.S. 398 (2013), the government assured the Court that "aggrieved persons" subject to FISA surveillance would receive notice. *See* Br. for Petitioner, *Amnesty Int'l*, 2012 WL 3090949, at *8; Tr. of Oral Argument at 4-5, *available at* http://www.supremecourt.gov/oral_arguments/argument_transcripts/2012/11-1025.pdf. Those representations were false. Instead, DOJ had adopted a practice "of not disclosing links" to Section 702 surveillance in criminal cases—a practice the Solicitor General later determined had "no legal basis." Charlie Savage, *Door May Open for Challenge to Secret Wiretaps,* N.Y. TIMES (Oct. 16, 2013). It was only after Snowden's revelations that the major discrepancy between the government's practice in Section 702 cases and what it told the Supreme Court was discovered. *Id.*

(10th Cir. 2021), *pet. for cert. docketed*, No. 22-5188 (U.S. July 26, 2022).[23] But to date—and despite conducting Upstream surveillance for well over a decade—the government has never provided notice to a criminal defendant that information specifically obtained or derived from Upstream was used in their prosecution.

Notice to criminal defendants has been more common in cases where the government used evidence derived from surveillance under Title I of FISA (under which the government may obtain individualized FISC orders to target U.S. persons). But here, too, there are questions about whether the government is at times engaging in parallel construction to avoid its notification obligation.[24] In *United States v. Osseily,* No. 8:19-cr-00117-JAK-1 (C.D. Cal.), for instance, the defendant received no notice of FISA surveillance, and

---

[23] In total, *amici* are aware of fewer than ten prosecutions where notice of Section 702 surveillance has been provided. *See United States v. Mohamud,* No. 10-cr-00475 (D. Or. Nov. 19, 2013) (ECF 486); *United States v. Hasbajrami,* No. 11-cr-00623 (E.D.N.Y. Feb. 24, 2014) (ECF 65); *United States v. Khan,* No. 12-cr-00659 (D. Or. Apr. 3, 2014) (ECF 59); *United States v. Mihalik,* No. 11-cr-00833 (C.D. Cal. Apr. 4, 2014) (ECF 145); *United States v. Zazi,* No. 09-cr-00663 (E.D.N.Y. July 27, 2015) (ECF 59); *United States v. Al-Jayab,* No. 16-cr-00181 (N.D. Ill. Apr. 8, 2016) (ECF 14); *United States v. Mohammad,* No. 15-cr-00358 (N.D. Ohio Dec. 21, 2015) (Dkt. Nos. 27-30).

[24] *See* Human Rights Watch, *Dark Side: Secret Origins of Evidence in US Criminal Cases* (Jan. 9, 2018), *available at* https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases.

learned that he had been subject to such surveillance only through discovery.[25]

Even when notice of FISA surveillance is given, defendants are still precluded from meaningfully challenging the surveillance used against them. Critically, the government refuses to provide defendants with necessary information about the surveillance, including FISC applications and orders. Indeed, in FISA's 44-year history, *no* criminal defendant has *ever* been allowed to review the FISA materials used to authorize their surveillance. *See* David S. Kris & J. Douglas Wilson, 1 NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 30:7 (3d ed. 2019). This lack of access renders challenges an exercise in futility.

Finally, even if every defendant subject to FISA surveillance received notice and had full access to the necessary materials, this would provide no remedy to the far larger number of individuals who are surveilled but never prosecuted. *See United States v. U.S. Dist. Court,* 407 U.S. 297, 318 (1972) ("post-surveillance review would never reach the surveillances which failed to result in prosecutions"). In 2021, the government provided notice of its intent to use FISA evidence in only five criminal proceedings. ODNI, *Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities (Calendar*

---

[25] *See* Br. of *Amici Curiae* ACLU and ACLU of Southern California in Support of Defendant's Motion for Disclosure of FISA-Related Material, *United States v. Osseily,* No. 8:19-cr-00117-JAK-1 (C.D. Cal. Jan. 28, 2020) (ECF 78).

Year 2021) at 31 (Apr. 2022).[26] During that same year, the government "targeted" 232,432 individuals under Section 702. ODNI (2021) at 17. Of course, the number of untargeted individuals swept up in that surveillance, which would include anyone who communicates with a target, is greater still. *See* Barton Gellman et al., *In NSA-Intercepted Data, Those Not Targeted Far Outnumber The Foreigners Who Are,* WASH. POST (July 5, 2014).

Thus, challenges to FISA surveillance—and particularly Section 702 surveillance—in criminal cases are both vanishingly rare and ineffective. The limitations of criminal prosecution challenges to FISA surveillance further underscore the need for this Court's intervention to preserve civil litigants' ability to seek judicial review of that surveillance.

CONCLUSION

The avenues for judicial review of FISA surveillance that exist outside of civil litigation—FISC proceedings and suppression efforts in criminal prosecutions—do not function as reliable checks on the government. Access to the courts through civil litigation is thus a vital safeguard for the vindication of constitutional rights implicated by foreign intelligence surveillance.

To preserve this safeguard, it is critical that the Court grant certiorari in this case. Only this Court can settle the questions now before it: *first*, whether the state secrets privilege articulated in *Reynolds* and *General Dynamics* authorizes courts to dismiss actions where plaintiffs can prove their case without

---

[26] *Available at* https://www.intelligence.gov/assets/documents/702%20Documents/statistical-transparency-report/2022_IC_Annual_Statistical_Transparency_Report_cy2021.pdf.

reliance on privileged evidence; and *second*, if the privilege does so authorize courts, whether a court may do so without first determining ex parte and in camera whether the privileged evidence establishes a valid defense. In our view, the lower court's conception of the state secrets privilege is fundamentally incorrect. Unless this Court rights the ship, there will soon be few, if any, effective means of checking unconstitutional abuses of the government's foreign intelligence surveillance authorities.

Respectfully submitted.

CHRIS SWIFT
Davis Wright Tremaine LLP
1300 SW Fifth Avenue
Suite 2400
Portland, OR 97201

ELIZABETH GOITEIN
Brennan Center for Justice at NYU School of Law
1140 Connecticut Ave. NW
Suite 1150
Washington, DC 20036

DAVID M. GOSSETT
Counsel of Record
MEENAKSHI KRISHNAN
Davis Wright Tremaine LLP
1301 K Street NW
Suite 500 East
Washington, DC 20005
(202) 973-4200
davidgossett@dwt.com

Counsel for Amici Curiae

SEPTEMBER 2022