No. 20-828

IN THE

Supreme Court of the United States

FEDERAL BUREAU OF INVESTIGATION, *et al.*,
Petitioners,

v.

YASSIR FAZAGA, *et al.*,
Respondents.

On Writ of Certiorari to the to the
United States Court of Appeals for the Ninth Circuit

BRIEF OF THE BRENNAN CENTER FOR JUSTICE, DUE PROCESS INSTITUTE, ELECTRONIC PRIVACY INFORMATION CENTER, FREEDOMWORKS FOUNDATION, AND TECHFREEDOM AS *AMICI CURIAE* IN SUPPORT OF RESPONDENTS YASSIR FAZAGA, *ET AL.*

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
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

CONSTITUTIONAL PROVISIONS

FEDERAL STATUTES

RULES

OTHER AUTHORITIES

INTEREST OF THE *AMICI CURIAE*

This brief is submitted jointly by the Brennan Center for Justice, Due Process Institute, Electronic Privacy Information Center (EPIC), FreedomWorks Foundation, and TechFreedom as *amici curiae* in support of respondents Yassir Fazaga, *et al.*[1]

Amicus curiae 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.

Amicus curiae Due Process Institute is a nonprofit, bipartisan, public interest organization that works to honor, preserve, and restore procedural fairness in the criminal justice system because due process is the guiding principle that underlies the

---

[1] Pursuant to Rule 37.6, *amici* affirm that no counsel for any party authored this brief in whole or in part, and no person or entity other than *amici* or their counsel made a monetary contribution to fund the preparation or submission of this brief. All parties have provided written consent to the filing of this *amicus* brief.

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

Constitution's solemn promises to "establish justice" and to "secure the blessings of liberty." U.S. Const., preamble. This case is of significant concern to the Institute because of the fundamental importance of protecting the people against unconstitutional governmental overreach via the use or abuse of its foreign intelligence surveillance authorities.

Amicus curiae 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 in the information age. EPIC has pushed for decades to increase oversight of national security surveillance and to halt unlawful expansions that violate individual rights. Following passage of the USA PATRIOT Act, EPIC fought for public access to records about the government's expansive assertion of surveillance authority,[3] and successfully sued for records concerning the warrantless wiretapping program, *EPIC* v. *DOJ*, 416 F. Supp. 2d 30 (D.D.C. 2006), and records about warrantless surveillance carried out under the FISA "pen register" authority, *EPIC* v. *DOJ*, 296 F. Supp. 3d 109 (D.D.C. 2017). EPIC brought the first challenge to the NSA telephone record collection program in this Court, *In re EPIC*, 134 S. Ct. 638 (2013), and filed an *amicus* brief in the Court concerning the ability of individuals to challenge national security surveillance. *Clapper* v. *Amnesty Int'l USA*, 568 U.S. 398 (2013). EPIC was also selected as the public interest representative to provide a counterbalancing perspective on U.S. surveillance remedies to the Court of Justice for the European Union in *Data Protection Commissioner* v.

---

[3] See EPIC, *USA Patriot Act* (2018), *available at* https://epic.org/privacy/terrorism/usapatriot/.

Facebook Ireland Ltd. (Schrems II), Case C-311/18, ECLI:EU:C:2020:559 (July 16, 2020).

Amicus curiae 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, *Paul* v. *Obama*, No. 14-cv-262 (D.D.C. filed Feb. 18, 2014).

Amicus curiae 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

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. Congress enacted FISA to provide judicial review of foreign surveillance efforts. Experience has shown, however, that the judicial review mechanisms established under FISA are largely inadequate—and in this litigation, the

government seeks to narrow the scope of judicial review under FISA even further. To assist the Court, in this brief we focus primarily on the ways in which FISA's other judicial review mechanisms have fallen short, thus underscoring the importance of civil litigation—which the government would effectively take off the table through its interpretation of 50 U.S.C. 1806(f).

I. FISA generally requires the government to obtain authorization from the Foreign Intelligence Surveillance Court (FISC) before conducting foreign intelligence surveillance that targets U.S. persons or takes place inside the United States. 50 U.S.C. 1803. But FISA establishes a largely non-adversarial ex parte process for reviewing foreign intelligence surveillance applications, *ibid.*, which has not provided a meaningful opportunity for judicial review.[4] One-sided procedures are inherently less reliable, and this problem is compounded when the government all too often submits inaccurate or misleading information to the FISC. Predictably, this has resulted in at least one high-profile instance of improperly authorized FISA surveillance. See Part I, *infra*.

II. Defendants may also 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 the government has stymied attempts by criminal

[4] Another FISA provision, Section 702, dispenses with even these minimal protections, permitting the government to intercept billions of communications—including communications between foreign targets and Americans—without any individualized court review or approval of the targets of the surveillance. 50 U.S.C. 1881a.

defendants to meaningfully challenge FISA surveillance, often evading FISA's judicial review provisions in criminal cases—even though those provisions already slant strongly in the government's favor. Moreover, these provisions cannot reliably check government abuses because they apply only where the government chooses to initiate a criminal prosecution. Where, as here, the government engages in surveillance but does not prosecute the targets of that surveillance, these provisions provide no basis for challenging the lawfulness of the government's conduct. See Part II, *infra*.

III. Finally, plaintiffs may seek judicial review of FISA surveillance by bringing a claim for damages under 50 U.S.C. 1810. And in the course of such litigation or any other legal proceedings, plaintiffs may move to "discover [or] obtain * * * evidence or information obtained or derived from electronic surveillance." 50 U.S.C. 1806(f). If the Attorney General files an affidavit that disclosure of the materials would harm national security, the court must undertake its own review of those materials to determine "whether the surveillance of the aggrieved person was lawfully authorized and conducted." *Ibid*. Congress intended for civil litigation to play an important role in protecting against improper FISA surveillance. By adopting these provisions, Congress displaced the federal common law in the field—namely, the state secrets privilege. Although the procedures contained in Section 1806(f) themselves can present a significant barrier to success in civil litigation, as they permit the court to review the materials in camera and ex parte and permit disclosure to the plaintiffs "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance," they are designed to allow

a case to proceed. *Ibid.* Thus, where a plaintiff challenges FISA surveillance in a civil case and the government claims state secrets are in jeopardy, the proper course is for the court to review the matter under 50 U.S.C. 1806(f).

Petitioners and their supporting Respondents seek to vitiate this final form of judicial oversight by contending that review under 50 U.S.C. 1806(f) is unavailable to plaintiffs seeking discovery in civil litigation. According to the government, only the judicially created state secrets privilege applies to civil challenges to FISA surveillance, and it requires dismissal of any claim that depends on evidence deemed to constitute a state secret.

Litigants' ability to obtain judicial review of FISA surveillance through civil cases is not only authorized by Congress, it is an essential bulwark against government overreach that must be strengthened rather than undermined. Applying the state secrets privilege to deny otherwise meritorious claims would only compound the injustice suffered by the victims of illegal surveillance. Congress expressly intended civil litigation to serve as a check on FISA abuses. See Part III, *infra*.

Accordingly, the Court should affirm the Ninth Circuit's decision so that the plaintiffs in this case may attempt to vindicate their rights. A ruling that the government can evade FISA's provision for civil lawsuits by invoking the common-law state secrets privilege to trump the carefully designed statutory provisions contained in Section 1806(f) would effectively eliminate one of the few means for protection against government overreach that currently exists.

ARGUMENT

I. FISC Proceedings Authorizing Foreign Intelligence Surveillance Do Not Adequately Protect Against Government Abuses.

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. 1803. But this process provides insufficient protection 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." *Ibid.* The risks of ex parte proceedings—one-sided, inaccurate factual presentations and distorted legal outcomes—have materialized, time and time again, in proceedings before the FISC.

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). And, 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 all the hallmarks of our adversarial system. And Congress's efforts in 2015 to make FISC proceedings more adversarial are far from sufficient.

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. 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 and programmatic surveillance techniques—techniques that presented sophisticated technical questions; complex and novel questions of federal statutory and constitutional law; and, at times, 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.

Congress amended FISA in 2015 to create a presumption that FISC judges should appoint *amici curiae* to assist the court's consideration of cases that present "a novel or significant interpretation of the law." See 50 U.S.C. 1803(i)(2)(A). But this *amicus* provision still does not guarantee an adversarial process. Among other problems, the FISC can decline to appoint *amici* if it determines that such appointment is "not appropriate," *ibid.*; and even when appointed, *amici* are not required to take positions in opposition to those of the government and therefore often 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 coincided with another troubling development: increasing evidence that the government was presenting false or misleading information to the FISC with its surveillance applications.

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—of 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; and this, in turn, led the court to authorize

surveillance based on incorrect or incomplete understandings of the programs. Often, the misrepresentations had the effect of concealing the government's failure to comply with the law or with court-imposed rules for the surveillance.

The first of these programs—the government's mass surveillance of domestic internet metadata—was marked by a "history of material misstatements" about the program's operation and repeated "noncompliance" with the FISC's orders. *[Redacted],* No. PR/TT [Redacted], at 72 (FISC [date redacted]).[5] Those misrepresentations led to frequent compliance problems. For years, the government "exceeded the scope of authorized acquisition continuously" under the FISC's supervision. *Id.* at 2-3. These were no mere technical violations, either: "[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 Mar. 2, 2009).[6] 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's operation. *Id.*

---

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

[6] *Available at* https://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf; see also *id.* at 14 ("historical record of non-compliance").

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 surveillance 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, on multiple, separate occasions, the government provided materially incomplete or misleading information to the FISC about its Section 702 surveillance. 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 one of its Section 702 collection methods was "fundamentally different from what the Court had been led to believe." *[Redacted],* No. [Redacted], at 28 (FISC Oct. 3, 2011).[7] 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 ha[d] disclosed a substantial misrepresentation regarding the scope of a major collection program." *Id.* at 16 n.14.

The government later revealed that it had retained improperly collected communications for years after it was required to purge them. The FISC

---

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

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).[8] 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 the government's implementation of Section 702. *[Redacted],* No. [Redacted] at 19, (FISC Apr. 26, 2017).[9] 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).[10] And earlier this year, the government released a 2020 FISC opinion in which the court recounted a "particularly concerning" "system failure" that resulted in noncompliance with a court-imposed documentation requirement, which went "undetected

---

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

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

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

or unreported for nearly a year." FISC. *[Redacted],* No. [Redacted] (FISC Nov. 18, 2000).[11]

The government's misrepresentations to the FISC are not limited to the operation of its mass surveillance programs; instead, all types of proceedings before the FISC appear to be afflicted with inaccuracies and errors. In December 2019, a report from the Department of Justice's Office of Inspector General (IG) reviewed four FISA applications submitted as part of the FBI's "Crossfire Hurricane" 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).[12] 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, in turn, 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,

---

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

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

at 2-3 (FISC Dec. 17, 2019).[13] In response to the IG report, 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).[14]

And, finally, the IG released initial findings in 2020 based on its review of the FBI's compliance with the "Woods Procedures"—procedures implemented by the FBI to ensure the accuracy of facts submitted in surveillance applications to the FISC. 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* (Mar. 2020).[15] The IG reviewed "a judgmentally selected sample of 29 [FISA] applications relating to U.S. Persons and involving both counterintelligence and counterterrorism investigations." *Id.* at 2. Of those, 25 contained "apparent errors or inadequately supported facts." *Id.* at 3. For four FISA applications, the FBI could not locate the files containing the requisite

---

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

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

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

documentation. *Id.* at 2-3. And for three of those four missing files, the FBI "did 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).[16]

It is therefore no wonder that 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).[17] 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 surveillance applications. *[Redacted],* No. [Redacted], at 13-14 (FISC [Date Redacted]).[18]

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

As we have discussed, the FISC reviews FISA applications through a non-adversarial process in which the government almost always appears ex parte and exhibits "a chronic tendency" to provide misleading information. It should therefore come as no surprise that this process does not consistently yield fair and reliable outcomes.

---

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

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

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

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).[19] Section 215 provided a statutory basis for the government to apply to the FISC, ex parte, and obtain an order compelling 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 is 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 call records of calls made to and from Americans.

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,

---

[19] Section 215 amended FISA's business records provision, 50 U.S.C. 1861. This provision has subsequently been amended to specifically address the collection of call records under FISA. See USA FREEDOM Act, Pub. L. 114-23, 129 Stat. 268 (2015) (amending 50 U.S.C. 1861). Nevertheless, the authority is still typically referred to as "Section 215."

2006).[20] 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), that specifically governs 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).[21]

In fact, the FISC did not undertake a full substantive review of 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 (FISC Aug. 29, 2013).[22] 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, *ibid.*, two years 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.

---

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

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

[22] *Available at* https://www.fisc.uscourts.gov/sites/default/files/BR%2013-109%20Order-1.pdf.

Supp. 2d 1 (D.D.C. 2013), *vacated on standing grounds and remanded,* 800 F.3d 559 (D.C. Cir. 2015).

In short, relying on incomplete information from the government and without conducting any substantial legal analysis, the FISC allowed the government to collect billions of call records under a mass surveillance program of dubious legality at best. 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 equally present when the FISC reviews individual surveillance applications, underscoring the inadequacy of FISC review as a protection against unlawful surveillance.

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

In criminal prosecutions, initial ex parte warrant proceedings are tolerated because later safeguards exist—searches can be challenged, facts can be contested, affiants can be impeached. But criminal defendants whose prosecutions are based on evidence derived from FISA surveillance have been unable to meaningfully challenge the surveillance that contributed to their prosecution.

One serious impediment to these FISA challenges is that the government rarely provides notice to the target of surveillance. FISA requires that the government provide notice when it intends to use evidence "obtained or derived from" FISA surveillance against an "aggrieved person." 50 U.S.C. 1806(c). The aggrieved person may then move to suppress evidence obtained through unauthorized surveillance. 50

U.S.C. 1806(e). But the government has found various ways to avoid this requirement.

In the first five years the government conducted Section 702 surveillance, for example, 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 of unilaterally and systematically 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*, at 2283.[23]

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

---

[23] In its briefs and at oral argument in *Clapper* v. *Amnesty International USA*, 568 U.S. 398 (2013), the government assured the Court that "aggrieved persons" subject to surveillance would receive notice that FISA surveillance had occurred. 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, the Justice Department 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), *available at* https://www.nytimes.com/2013/10/17/us/politics/us-legal-shift-may-open-door-for-challenge-to-secret-wiretaps.html. It was only after the revelations of former NSA-contractor Edward Snowden that the major discrepancy between the government's practice in Section 702 cases and what it told the Supreme Court was discovered. *Ibid.*

(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[.]").[24]

Notification of 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). Here, too, however, there are questions about whether the government is at times engaging in "parallel construction" to avoid its notification obligation.[25] In *United States* v. *Osseily*, No. 8:19-cr-00117-JAK-1 (C.D. Cal.) (pending), for instance, the defendant received no notice of FISA surveillance, and learned that he had been subject to such surveillance only through discovery.[26]

---

[24] In total, we 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) (Dkt. No. 486); *United States* v. *Hasbajrami*, No. 11-cr-623 (E.D.N.Y. Feb 24, 2014) (Dkt. No. 65); *United States* v. *Khan*, No. 12-cr-00659 (D. Or. Apr. 3, 2014) (Dkt. No. 59); *United States* v. *Mihalik*, No. 11-cr-833 (C.D. Cal. Apr. 4, 2014) (Dkt. No. 145); *United States* v. *Zazi*, No. 09-cr-00663 (E.D.N.Y July 27, 2015) (Dkt. No. 59); *United States* v. *Al-Jayab*, No. 16-cr-181 (N.D. Ill. Apr. 8, 2016) (Dkt. No. 14); *United States* v. *Mohammad*, No. 15-cr-00358 (N.D. Ohio Dec. 21, 2015) (Dkt. No. 27).

[25] 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.

[26] See Br. of *Amici Curiae* American Civil Liberties Union and American Civil Liberties Union of Southern California in Support of Defendant's Motion for Disclosure of FISA-Related

Moreover, even if the government provided proper notice of FISA surveillance in every criminal prosecution where such surveillance had occurred, this would provide no remedy to the far larger number of individuals who have been improperly surveilled but never prosecuted. See *United States* v. *U.S. Dist. Court,* 407 U.S. 297, 318 (1972) (explaining that, in most circumstances, "post-surveillance review would never reach the surveillances which failed to result in prosecutions").

In short, a vanishingly small proportion of those surveilled under FISA receive notice as part of a criminal proceeding. In 2019, the government provided notice of its intent to use FISA evidence in 7 criminal proceedings. ODNI, *Statistical Transparency Report Regarding the Intelligence Community Use of National Security Surveillance Authorities (Calendar Year 2020)* at 27.[27] During the same year, the government reported surveilling an estimated 204,968 targets under Section 702 and 1,059 targets under its other FISA authorizations. See *id.* at 10, 16, 29, 32. Of course, the number of untargeted individuals swept up in that surveillance web is greater still. See Barton Gellman, Julie Tate & Ashkan Soltani, *In NSA-Intercepted Data, Those Not Targeted Far Outnumber The Foreigners Who Are,* Wash. Post (July 5, 2014).[28]

Material, *United States* v. *Osseily*, No. 8:19-cr-00117-JAK-1 (C.D. Cal. Jan. 28, 2020) (Dkt. No. 78).

[27] *Available at* https://www.dni.gov/files/CLPT/documents/2021_ASTR_for_CY2020_FINAL.pdf.

[28] *Available at* https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-out number-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html. See also Barton Gellman, *How 160,000 Intercepted Communications Led To Our Latest*

Finally, even in the small number of cases in which criminal prosecutions occur and 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 forty-year history, not a single criminal defendant has 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). These challenges will continue to be exercises in futility so long as the government bars defendants from even seeing the relevant materials.

III. The Ability To Challenge FISA Surveillance Through Civil Litigation Is Necessary To Prevent Government Abuses.

Congress never intended the FISC to have a monopoly on judicial review of FISA surveillance. Instead, Congress expected the adversarial process in *both* criminal prosecutions *and* civil litigation to function as a check on FISA abuses. As we just discussed, criminal prosecutions have not served that function. It is thus all the more critical that civil litigation be available to fill the void. Allowing the government to invoke the state secrets privilege to circumvent judicial review under FISA is inconsistent

---

NSA Story, Wash. Post (July 11, 2014), *available at* https://www.washingtonpost.com/world/national-security/your-questions-answered-about-the-posts-recent-investigation-of-nsa-surveillance/2014/07/11/43d743e6-0908-11e4-8a6a-19355c7e870a_story.html.

with both congressional intent and the preservation of constitutional liberties.

A. Congress authorized judicial review of FISA surveillance in all civil cases involving evidence obtained under FISA.

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

In addition, through FISA, Congress created a mandatory process by which the federal courts, applying appropriate security procedures, must evaluate the lawfulness of foreign intelligence surveillance, where at issue, in legal proceedings of all types. See 50 U.S.C. 1806(f). FISA's Section 1806(f) procedures apply to any challenge brought under other subsections of Section 1806 *or* "pursuant to any other statute or rule * * * before any court * * * to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter[.]" *Ibid.* Under Section 1806(f), "if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States," then the court must review "in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." *Ibid.* However, Section 1806(f) permits disclosure of materials where

"necessary to make an accurate determination of the legality of the surveillance." *Ibid.*

As the Ninth Circuit correctly held, by Section 1806(f)'s plain terms—and "[c]ontrary to the Government's contention"—these "procedures are to be used when an aggrieved person affirmatively challenges, in any civil case, the legality of electronic surveillance or its use in litigation, whether the challenge is under FISA itself, the Constitution, or any other law." Pet. App. 64a-65a; but see *Wikimedia Found.* v. *Nat'l Sec. Agency*, __ F.4th __, 2021 WL 4187840 (4th Cir. Sept. 15, 2021). Any other reading of the statute would run roughshod over the statute's language and Congress's intent.

B. The state secrets privilege does not allow the government to circumvent FISA and prevent judicial review of the legality of its surveillance activities.

Petitioners and their supporting Respondents contend that Section 1806(f) applies only where "the government affirmatively seeks to 'use or disclose' FISA-obtained or FISA-derived evidence or information * * *." Pet. Br. 36. As they would have it, in all other cases the government can invoke the state secrets privilege and mandate dismissal whenever the government claims that national security would be harmed by disclosure of evidence necessary to a plaintiff's claim. *Id.* at 11–12, 26.

This argument would largely nullify the only mechanism by which aggrieved persons can affirmatively challenge FISA surveillance. Especially given the limitations of judicial review by the FISC and in criminal cases, this theory would leave individuals with little protection against unlawful surveillance.

Nothing in the broad language of Section 1806(f) limits its reach to cases in which the government seeks to introduce FISA evidence. To the contrary, as the Ninth Circuit explained, Congress adopted FISA in order to displace the state secrets privilege in the field of electronic surveillance. "In striking a careful balance between assuring the national security and protecting against electronic surveillance abuse," the court of appeals noted, "Congress carefully considered the role previously played by courts, and concluded that the judiciary had been unable effectively to achieve an appropriate balance through federal common law[.]" Pet. App. 54a. Congress concluded that "the development of standards and restrictions by the judiciary with respect to electronic surveillance for foreign intelligence purposes accomplished through case law threatens both civil liberties and the national security." *Id.* at 54a-55a (quoting H. Rep. No. 95-1283, pt. 1, at 21).

This "careful balance" depends upon the ability of private litigants to bring civil actions against the government to "protect[] against electronic surveillance abuse." *Ibid.* FISA reflects Congress's considered judgment that civil litigants can and should be allowed to challenge FISA surveillance practices. Ignoring the plain language of 50 U.S.C. 1806(f) in favor of Petitioner's erroneous conception of the state secrets privilege would vitiate Congress's intent and undermine the accountability needed to safeguard Americans' liberty and privacy.

CONCLUSION

The avenues for judicial review of FISA surveillance that exist outside of civil litigation—proceedings before the FISC and to suppress evidence in criminal prosecutions—are unreliable and are not

functioning as Congress intended. Access to the courts through civil litigation is thus a critical safeguard for the vindication of constitutional rights implicated by foreign intelligence surveillance. The Ninth Circuit's ruling should therefore be affirmed, and this case should be remanded to the district court for a decision on the merits.

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
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 2021