Case No. 20-01191

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

WIKIMEDIA FOUNDATION,

Plaintiff-Appellant,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants-Appellees.

BRIEF OF AMICI CURIAE AMERICANS FOR PROSPERITY FOUNDATION, BRENNAN CENTER FOR JUSTICE, ELECTRONIC FRONTIER FOUNDATION, ELECTRONIC PRIVACY INFORMATION CENTER, FREEDOMWORKS FOUNDATION, AND TECHFREEDOM IN SUPPORT OF PLAINTIFF-APPELLANT AND REVERSAL

On Appeal from the U.S. District Court
for the District of Maryland at Baltimore
Case No. 1:15-cv-00662-TSE
U.S. District Court Judge T.S. Ellis, III

Eric R. Bolinder
AMERICANS FOR PROSPERITY FOUNDATION
1310 N. Courthouse Rd., Suite 700
Arlington, VA 22201
(571) 329-3324
ebolinder@afphq.org

Sophia Cope
Mark Rumold
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
(415) 436-9333
sophia@eff.org

Counsel for Amici Curiae

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

DISCLOSURE STATEMENT

- In civil, agency, bankruptcy, and mandamus cases, a disclosure statement must be filed by **all** parties, with the following exceptions: (1) the United States is not required to file a disclosure statement; (2) an indigent party is not required to file a disclosure statement; and (3) a state or local government is not required to file a disclosure statement in pro se cases. (All parties to the action in the district court are considered parties to a mandamus case.)
- In criminal and post-conviction cases, a corporate defendant must file a disclosure statement.
- In criminal cases, the United States must file a disclosure statement if there was an organizational victim of the alleged criminal activity. (See question 7.)
- Any corporate amicus curiae must file a disclosure statement.
- Counsel has a continuing duty to update the disclosure statement.

No. 20-01191 Caption: Wikimedia Foundation v. National Security Agency, et al

Pursuant to FRAP 26.1 and Local Rule 26.1,

Americans for Prosperity Foundation, Brennan Center for Justice, Electronic Frontier Foundation,
(name of party/amicus)

Electronic Privacy Information Center, FreedomWorks Foundation, and TechFreedom

who is amici curiae, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☐ YES ☑ NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation? ☐YES ☑NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐YES ☑NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐YES ☑NO
If yes, the debtor, the trustee, or the appellant (if neither the debtor nor the trustee is a party) must list (1) the members of any creditors' committee, (2) each debtor (if not in the caption), and (3) if a debtor is a corporation, the parent corporation and any publicly held corporation that owns 10% or more of the stock of the debtor.

7. Is this a criminal case in which there was an organizational victim? ☐YES ☑NO
If yes, the United States, absent good cause shown, must list (1) each organizational victim of the criminal activity and (2) if an organizational victim is a corporation, the parent corporation and any publicly held corporation that owns 10% or more of the stock of victim, to the extent that information can be obtained through due diligence.

Signature: /s/ Sophia Cope Date: July 8, 2020

Counsel for: Electronic Frontier Foundation

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Legislative Materials

Other Authorities

STATEMENT OF INTEREST[1]

Amicus curiae Americans for Prosperity Foundation ("AFPF") is a 501(c)(3) nonprofit organization committed to educating and training Americans to be courageous advocates for the ideas, principles, and policies of a free and open society. Some of those key ideas include the separation of powers and constitutionally limited government. As part of this mission, AFPF appears as amicus curiae before state and federal courts. AFPF has a particular interest in this case because of its consistent body of work promoting tech entrepreneurship and protecting the privacy interests of American consumers and businesses.

Amicus curiae the Brennan Center for Justice at NYU School of Law[2] is a non-partisan public policy and law institute focused on fundamental issues of democracy and justice. The Center's Liberty and National Security (LNS) 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 LNS Program's main areas of research and

[1] No party's counsel authored this brief in whole or in part. Neither any party nor any party's counsel contributed money that was intended to fund preparing or submitting this brief. No person other than amici, their members, or their counsel contributed money that was intended to fund the preparing or submitting of this brief. All parties have consented to the filing of this brief.

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

advocacy is foreign intelligence surveillance. LNS Program staff have produced in-depth research reports on the topic (including a 2015 report, *What Went Wrong With the FISA Court*, that focuses primarily on Section 702); submitted amicus briefs in connection with FISA litigation; and testified before the Senate and House Judiciary Committees on multiple occasions regarding Section 702 and other aspects of FISA.

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 civil liberties issues and to protect privacy, the First Amendment, and other constitutional values. EPIC routinely participates as amicus curiae before federal courts in cases concerning the impact of electronic surveillance on civil liberties. *See, e.g.*, *Carpenter v. United States*, 138 S. Ct. 2206 (2018); *Riley v. California*, 314 S. Ct. 2473 (2014); *Smith v. Obama*, 816 F.3d 1239 (9th Cir. 2016). EPIC brought the first challenge to the NSA telephone record collection program in the U.S. Supreme Court and continues to participate as amicus in challenges to NSA surveillance. *In re EPIC*, 134 S. Ct. 638 (2013); *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013).

Amicus curiae Electronic Frontier Foundation ("EFF") is a member-supported, non-profit organization that has worked for 30 years to ensure that technology supports freedom, justice, and innovation for all people of the world.

For nearly two decades, EFF has participated, either directly or as amicus, in litigation to ensure our nation's national security surveillance programs operate in accordance with federal laws and the Constitution. Since 2009, EFF has represented plaintiffs in a civil case challenging the NSA's Upstream surveillance. *See Jewel v. NSA*, No. 19-16066 (9th Cir. filed May 21, 2019). EFF has also served as amicus in a variety of cases involving FISA surveillance. *See, e.g.*, *United States v. Mohamud*, 843 F.3d 420 (9th Cir. 2016); *United States v. Daoud*, 755 F.3d 479 (7th Cir. 2014); *United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019); *United States v. Gartenlaub*, 751 Fed. App'x 998 (9th Cir. 2018).

Amicus curiae FreedomWorks Foundation is a non-profit, non-partisan 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 since 2013 in education about the dangers 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 NSA mass metadata collection, *Paul v. Obama*, No. 14-cv-262, (D.D.C. filed Feb. 18, 2014).

Amicus curiae TechFreedom is a non-profit, non-partisan 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 privacy rights protected by the Fourth Amendment, the crown jewel of American civil liberties.

INTRODUCTION

The government's foreign intelligence surveillance operates in ways our nation's founders could never have anticipated. This surveillance is fundamentally unlike anything the Supreme Court has ever reviewed—let alone countenanced. And the careful balance Congress sought to achieve by enacting the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1801, et seq., has now tipped too far in the government's favor.

Under Section 702 of FISA, 50 U.S.C. § 1881a, the government has intercepted literally billions of communications, including the communications of Americans, without any court reviewing or approving the individual targets of the surveillance. The government conducts so-called "Upstream" surveillance under Section 702, a technique which entails searching communications, including those of Americans, as they flow through the Internet backbone. Upstream surveillance presents a range of singular and significant constitutional questions—questions *no* court has ever fully addressed.

It is critical that those directly affected by mass foreign intelligence surveillance be able to obtain judicial review of these constitutional questions. But one-sided proceedings in the Foreign Intelligence Surveillance Court ("FISC") have failed to produce dependable legal outcomes. And the government has

stymied attempts by criminal defendants to meaningfully challenge FISA surveillance.

Amici represent a variety of political philosophies and approaches to advocacy, but we agree on this: FISA is broken. Given this breakdown, the ability of civil litigants, like Wikimedia, to challenge the NSA's Upstream surveillance is all the more critical.

Congress intended civil litigation to serve as a check on FISA abuses. The district court's decision should be reversed so that Wikimedia may do just that: receive a judgment on the merits on the legality of Upstream surveillance.

ARGUMENT

I. One-sided FISC proceedings are inadequate to fairly and accurately determine the legality of foreign intelligence surveillance programs.

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 proceedings before the FISC.

A. Ex parte proceedings, like those before the FISC, produce unreliable factual and legal determinations.

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).

Yet proceedings before the FISC typically lack all the hallmarks of our adversarial system. For nearly forty years—from the court's inception in 1978 until 2015[3]—almost *all* proceedings before the FISC were ex parte.[4]

Initially, the FISC considered government applications to conduct domestic

[3] In 2015, Congress saw fit to add some elements of the adversarial process to FISA. Congress amended FISA to allow FISC judges to 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). Notwithstanding this improvement, significant concerns still remain about the adequacy and function of FISA's amicus provision. *See, e.g.*, 166 Cong. Rec. S2410-2412 (daily ed. May 13, 2020) (statement of Sen. Leahy) (describing proposed amendments to FISA amicus provision). Among other problems, amici before the FISC 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.

[4] A limited number of exceptions exist. *See, e.g.*, *In re Directives*, 551 F.3d 1004 (FISCR 2008); *In re Sealed Case*, 310 F.3d 717 (FISCR 2002).

electronic surveillance of specific individuals for foreign intelligence purposes—a process designed to mirror the issuance of warrants and wiretaps in traditional criminal proceedings. *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.

B. The government has repeatedly provided the FISC with materially incomplete or misleading information, plaguing all aspects of FISA surveillance.

The FISC's consideration, ex parte, 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.

For example, the government has publicly disclosed 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 Collection of Tangible Things from [Redacted]*, No. BR 08-13, at 10 (FISC Mar. 2, 2009).[6] The government compounded its "historical record of noncompliance" 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*. 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

[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.

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—including the Upstream surveillance at issue here. 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).[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 has disclosed a substantial misrepresentation regarding the scope of a major collection program," *id.* at 16 n.14.

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

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).[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 Section 702 surveillance. *[Redacted]*, No. [Redacted] (FISC Apr. 26, 2017).[9] And yet another FISC opinion described "documented misunderstandings" of relevant FISC-imposed standards, that led to "broad and apparently suspicionless" searches and lengthy government "delays in reporting" violations to the FISC. *[Redacted]*, No. [Redacted] (FISC Oct. 18, 2018).[10]

---

[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.intel.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf.

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 Department of Justice, Office of Inspector General ("IG") report reviewed four FISA applications submitted as part of the FBI's "Crossfire Hurricane" investigation—an 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).[11] 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, at 2 (FISC Dec. 17, 2019). In response to the IG report, the FISC noted that the "frequency with which

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

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 2. *See also In re Accuracy Concerns Regarding FBI Matters Submitted to the FISC*, No. Misc. 19-02, at 1 (FISC Mar. 4, 2020).[12]

And, finally, earlier this year, the IG released preliminary findings 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* (March 2020).[13] The IG reviewed 29 FISA applications. *Id*. 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

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

[13] *Available at* https://oig.justice.gov/reports/2020/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 (FISC Apr. 3, 2020).[14]

It is no wonder, under these circumstances, 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).[15] 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]).[16]

---

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

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

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

C. The lack of an adversarial process and the government's provision of inaccurate and misleading information to the FISC have yielded unreliable legal outcomes.

It should come as no surprise that the adequacy of the FISC's decisions have suffered in light of the court's extensive ex parte operation and the government's repeated provision of incomplete or inaccurate information.

The FISC's consideration of the NSA's program of mass surveillance of domestic call records illustrates the problem. That program—which involved the collection of 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).[17] 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," like business records or documents, if the government could show those tangible things were relevant to an authorized counterterrorism, counterespionage, or foreign intelligence investigation.

Yet the government interpreted this statutory authority—which is explicitly no broader than a grand jury or similar subpoena authority, 50 U.S.C.

[17] 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."

§ 1861(c)(2)(D)—to allow the compelled disclosure of billions of call records of calls made to and from Americans.

Despite the obvious expansiveness of the government's interpretation of the statute, 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).[18] There was no accompanying legal analysis or opinion.

It took the government two years after the issuance of the FISC's bulk collection order to bring the court's attention to another statute, the Stored Communications Act, 18 U.S.C. § 2701, et seq. ("SCA")—a statute that specifically governs the disclosure of call records from telecommunications providers. *See In re Production of Tangible Things from [Redacted]*, No. BR 08-13 (FISC Dec. 12, 2008).[19] The SCA was plainly necessary to the FISC's

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

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

consideration of the program from the outset, but the government failed to raise it until nearly two years after the program began.

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. *Compare 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).[20] Not coincidentally, this review occurred shortly after the secrecy of the program was pierced by Edward Snowden's disclosures. And, notwithstanding this post hoc review, after little more than two years of public, adversarial testing of the substantive legal basis for the phone records program, two federal courts concluded the NSA's 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 and remanded*, 800 F.3d 559 (D.C. Cir. 2015).

But there is no better illustration of the limits of the FISC's review than Upstream surveillance. Indeed, compared even to other provisions of FISA, the FISC's review of Section 702—and, by extension, Upstream surveillance—is more "narrowly circumscribed." *In re Proceedings Required by § 702(i) of FISA*

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

Amendments Act, Misc. No. 08-01, 2008 WL 9487946, at 2 (FISC Aug. 27, 2008). And, despite annually reviewing the government's Section 702 surveillance for more than a decade, the FISC has never addressed—to amici's knowledge—the specific and threshold constitutional question presented by this case: whether the government violates the Fourth Amendment by scanning and searching Americans' communications, en masse, as those communications flow through the Internet backbone.

II. Judicial review, based on an adversarial process, does not reliably occur in FISA cases—even in criminal prosecutions.

In criminal prosecutions, initial ex parte 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—including Upstream surveillance—have been unable to meaningfully challenge the surveillance that contributed to their prosecution.

Notice that Section 702 surveillance was used in a criminal prosecution is exceedingly rare. FISA requires the government provide notice to parties to legal proceedings when it uses evidence "obtained or derived from" FISA surveillance. 50 U.S.C. § 1806(c). Yet, for the first five years the government conducted Section 702 surveillance, no defendant received notice. 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 Section 702 surveillance to be challenged. *See* Mondale, *No Longer a Neutral Magistrate* at 2283.[21]

The government ultimately notified a handful of defendants whose prosecutions involve 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. Nov. 19, 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[.]").[22]

---

[21] In its briefs and at oral argument in *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), the government assured the Supreme Court that "aggrieved persons" subject to surveillance would receive notice that FISA surveillance had occurred. *See* Br. for Petitioner, *Amnesty*, 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). 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. *Id.*

[22] 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) (Dkt. No. 486); *United States v. Hasbajrami*, No.

To date—and despite conducting Upstream surveillance for nearly two decades—the government has *never* provided notice to a criminal defendant that information obtained or derived from Upstream, specifically, was used in their prosecution.

Even when notice of FISA surveillance is given, defendants are still precluded from meaningfully challenging the surveillance used against them: the government refuses to provide them with necessary information about the surveillance, like 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).

Regardless, the handful of prosecutions in which notice of Section 702 surveillance has been provided—in total, fewer than 10—are dwarfed by the number of individuals surveilled under Section 702. According to the latest transparency report released by the Office of the Director of National Intelligence

---

11-cr-623 (E.D.N.Y. Feb 24, 2014) (Dkt. No. 65); *United States v. Khan*, No. 12-cr-00659 (D. Ore. 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 Jul. 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. Oh. Dec. 21, 2015) (Dkt. No. 27).

("ODNI"), the government "targeted" 204,968 individuals under Section 702 surveillance in 2019. ODNI, *Calendar Year 2019 Transparency Report* at 14.[23] But the number of untargeted individuals swept up in that surveillance web far outpaces even the hundreds of thousands of surveillance "targets." *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).[24]

Unless more "targets" are prosecuted for crimes, and unless the government unilaterally determines those defendants should receive notice, challenges to Section 702 surveillance in criminal cases will remain exceedingly rare. *See United States v. U.S. Dist. Court for E. Dist. Of Mich.*, 407 U.S. 297, 318 (1972) (finding that, in most circumstances, "post-surveillance review would never reach the surveillances which failed to result in prosecutions"). But those challenges will be

[23] *Available at* https://www.odni.gov/files/CLPT/documents/2020_ASTR_for_CY2019_FINAL.pdf. The number of annual targets has more than doubled in less than five years. *See id*.

[24] *Available at* http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-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 NSA Story*, Wash. Post (July 11, 2014), *available at* http://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.

exercises in futility if the government continues to bar defendants from seeing the relevant materials.

III. In civil cases challenging FISA surveillance, Congress intended for judicial review after an adversarial process.

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 described above, criminal prosecutions have not served that function. It is thus all the more critical that civil litigation, like this case, is allowed to fill the void.

Indeed, FISA's text represents an express Congressional purpose to allow 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.

More fundamentally, through FISA, Congress created a mandatory process by which the federal courts, applying appropriate security procedures, could evaluate the lawfulness of foreign intelligence surveillance in civil cases. *See* 50 U.S.C. § 1806(f). FISA's 1806(f) procedures apply in "any civil case" challenging the "legality of electronic surveillance or its use in litigation, whether the challenge is under FISA itself, the Constitution, or any other law." *Fazaga v. FBI*, 916 F.3d 1202, 1238 (9th Cir. 2019). And those procedures specifically anticipate the

involvement of the party challenging the surveillance. *See* 50 U.S.C. § 1806(f) (noting court's authority to order disclosure of FISA materials where necessary to "make an accurate determination of the legality of the surveillance").

In enacting FISA, Congress struck a "careful balance" between "assuring the national security and protecting against electronic surveillance abuse." *Fazaga*, 916 F.3d at 1233. FISA represents Congress's considered judgment that civil litigants can and should be allowed to challenge FISA surveillance practices.

CONCLUSION

The avenues for judicial review of FISA surveillance that exist outside of civil litigation—namely, proceedings before the FISC and 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 district court's judgment should therefore be reversed, and this case should be remanded to the district court for a decision on the merits.

Dated: July 8, 2020

Respectfully submitted,

/s/ Sophia Cope
Sophia Cope
Counsel of Record
Mark Rumold
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109

(415) 436-9333
sophia@eff.org
Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS PURSUANT TO FED. R. APP. P. 32(g)

Pursuant to Fed. R. App. P. 32(g), I certify as follows:

1. This Brief of Amicus Curiae Electronic Frontier Foundation in Support of Plaintiffs-Appellants and Reversal complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 4,766 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2016, the word processing system used to prepare the brief, in 14-point font in Times New Roman font.

Dated: July 8, 2020

/s/ Sophia Cope
Sophia Cope

Counsel of Record for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Fourth Circuit by using the appellate CM/ECF system on July 8, 2020.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: July 8, 2020

/s/ Sophia Cope
Sophia Cope

Counsel of Record for Amici Curiae