Case No. 15-2560

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

WIKIMEDIA FOUNDATION, et al.,

Plaintiffs-Appellants,

v.

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

Defendants-Appellees.

BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PLAINTIFFS-APPELLANTS

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

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

Counsel for Amicus Curiae

DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN LITIGATION

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *amicus curiae* the Electronic Frontier Foundation states that it does not have a parent corporation, and that no publicly held corporation owns 10 percent or more of the stock of *amicus*.

Dated: February 24, 2016

Respectfully submitted,

/s/ Sophia Cope

Sophia Cope
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Counsel for Amicus Curiae Electronic Frontier Foundation

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Constitutional Provisions

Foreign Intelligence Surveillance Court Opinions

Other Authorities

STATEMENT OF INTEREST[1]

EFF is a non-profit, member-supported civil liberties organization working to protect rights in the digital world. Founded in 1990, EFF has over 26,000 members across the United States. After nearly a decade of litigating national security mass surveillance cases, the Electronic Frontier Foundation ("EFF") has unique expertise to offer the Court as *amicus curiae* at a time when technological advances afford the government an unprecedented ability to pry into the private lives of innocent Americans.

In 2006, EFF filed *Hepting v. AT&T*, a class action challenging AT&T's participation in the NSA's surveillance of the companies' fiber optic Internet cables—a surveillance operation, now known as Upstream, at the heart of this case. *Hepting* was ultimately dismissed following Congress' grant of legal immunity to telecommunication providers as part of the FISA Amendments Act of 2008 ("FAA"), Pub. L. No. 110-261, 122 Stat. 2436, 2468 (July 10, 2008) (adding Foreign Intelligence Surveillance Act § 802, codified at 50 U.S.C. § 1885a). *Hepting*, 671 F.3d 881 (9th Cir. 2011). In 2008, on behalf of a similar class of AT&T customers based on similar allegations, EFF filed a new suit directly against the government—*Jewel v. NSA*, No. 08-cv-04373 (N.D. Cal. 2008). That case remains ongoing today.

[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 *amicus*, its members, or its counsel contributed money that was intended to fund preparing or submitting this brief. All parties have consented to the filing of this brief.

In addition to *Jewel*, EFF serves as counsel in *First Unitarian Church of Los Angeles v. NSA*, No. 13-cv-03287 (N.D. Cal. 2013), and *Smith v. Obama*, No. 14-35555 (9th Cir. 2014), both of which challenge the NSA's mass surveillance of domestic phone records; and was counsel in *Human Rights Watch v. DEA*, Case No. 2:15-cv-02573 (C.D. Cal. 2015), which challenged the DEA's mass surveillance of international phone records.

EFF served as counsel to *amici curiae* the American Booksellers Association, the American Library Association, the Association of Research Libraries, the Freedom to Read Foundation, and the International Federation of Library Associations and Institutions before the district court in this case.

INTRODUCTION

The Supreme Court did not intend *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013) ("*Amnesty*"), to place government mass surveillance programs outside the reach of judicial review.

Yet the district court's opinion has precisely that effect. Based almost entirely on *Amnesty*, it ignores the critical distinction between the Supreme Court's decision and the present case: Plaintiffs here plausibly allege *actual* incidents, both past and continuing, of government interception of their Internet communications. That this case concerns national security surveillance may complicate the proof of those claims, but it does not prevent it. And it certainly does not require a threshold dismissal.

The ability of civil litigants, like Plaintiffs, to challenge the NSA's "Upstream" surveillance program is particularly important given the failure of other avenues of legal review of surveillance under Section 702 of the Foreign Intelligence Surveillance Act ("Section 702"),[2] as identified by the *Amnesty* Court: review by the Foreign Intelligence Surveillance Court ("FISC"), by criminal defendants prosecuted using Section 702 evidence, or by electronic communications service providers. All have proven insufficient.

[2] Codified at 50 U.S.C. § 1881a (added by FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436, 2438 (July 10, 2008)).

A "federal court's obligation to hear and decide cases within its jurisdiction is virtually unflagging," *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 134 S. Ct. 1377, 1386 (2014) (internal citations and quotations omitted), and insulating government mass surveillance programs from judicial review—even those implicating national security—risks allowing the Executive to "switch the Constitution on or off at will." *Boumediene v. Bush*, 553 U.S. 723, 765 (2008).

The federal courts have jurisdiction to hear this case, and this Court should therefore allow it to proceed to a decision on the merits.

ARGUMENT

I. *AMNESTY* DOES NOT COMPEL THE DISMISSAL OF THIS CASE.

A. Plaintiffs That Allege a Concrete, Particularized, and Actual Injury in Fact Have Article III Standing to Challenge the Legality of the Government Conduct That Caused That Injury.

To have standing, a plaintiff must assert an "injury in fact" that is both "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992)). *See also Bostic v. Shaefer*, 760 F.3d 352, 370 (4th Cir. 2014); *Jewel v. NSA*, 673 F.3d 902, 908 (9th Cir. 2011).

Plaintiffs have done so here.

B. Plaintiffs' Plausible Allegations That Their Communications Have Actually Been Intercepted Distinguish This Case From Amnesty.

The district court's reliance on *Amnesty* to reach a contrary conclusion was wrong. Whereas *Amnesty* interpreted the "injury in fact" requirement in the context of a pre-enforcement challenge to a statute under which the government had not yet taken any action, the injury alleged in the present case arises from past and ongoing surveillance under an implemented statute.

Amnesty was a facial challenge to Section 702 of the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1881a, filed the day the law went into effect. 133 S. Ct. at 1146. The suit was filed before the government *even began* surveillance under the law. Thus, the plaintiffs could only allege "an objectively reasonable likelihood" that, "at some point in the future," "their communications will be acquired under § 1881a." *Id*. Little was known about the surveillance the government would implement under its new authority, save the generalities that could be gleaned from the face of the statute.

In a 5-4 decision, the Supreme Court tailored its "injury in fact" analysis to injury based on anticipated, future conduct. The Court thus took issue with the plaintiffs' failure to allege an injury that was "certainly impending" as it was only "based on potential future surveillance." *Id*. at 1150, 55.[3]

[3] Even in the context of pre-enforcement challenges, *Amnesty* does not require proof of certainty of harm, as the district court implied. As the Supreme Court recently unanimously reaffirmed in *Susan B. Anthony List*, the "certainly impending" standard is not the complete test, even in cases involving allegations of "imminent" future injury. Rather, it is just one way of demonstrating standing. A plaintiff has standing if "the threatened injury is certainly impending, *or* there is a

The plaintiffs' inability to allege that communications had actually been intercepted was critical to the Supreme Court's decision in *Amnesty*. As the Court noted, "respondents fail to offer any evidence that their communications have been monitored under § 1881a, a failure that substantially undermines their standing theory." *Amnesty*, 133 S. Ct. at 1148. Indeed, the *Amnesty* plaintiffs *could not* provide that evidence (or even make those allegations): the lawsuit was filed before government surveillance under Section 702 began. At best, the *Amnesty* plaintiffs could only allege that something might happen in the future.

In contrast, the very first paragraph of the complaint in this case contains what the Supreme Court found conspicuously absent in *Amnesty*:

> [T]he NSA is seizing Americans' communications en masse while they are in transit, and it is searching the contents of substantially all international text-based communications.

First Amendment Complaint ("FAC") ¶ 1. And the allegation—backed by government admissions and documentary evidence—is repeated throughout the complaint. *See* FAC ¶ 50 (Upstream surveillance "involves the surveillance of essentially *everyone's* communications") (emphasis in original); ¶ 56 ("[T]he government is seizing and searching Plaintiff's communications."). *See also* ¶¶ 57-67.

---

substantial risk that the harm will occur." *Susan B. Anthony List*, 134 S. Ct. at 2341 (internal quotations omitted; emphasis added) (citing *Amnesty*, 133 S.Ct. at 1147, 1150, n. 5). *See also Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 153-54 (2010) (finding standing based on a "substantial risk" that the harm would occur).

The district court failed to recognize this critical distinction, instead conflating the absence of conclusive proof of an injury with the absence of a plausibly alleged injury. But that "approach conflates the ultimate merits question . . . with the threshold standing determination." *Jewel*, 673 F.3d at 911 n. 5. At the motion to dismiss stage, standing requires only the presence of a plausible injury, and in this case Plaintiffs' allegations are sufficient.[4]

Not only are Plaintiffs' allegations of harm based on past and ongoing government conduct, the allegations are also more concretely grounded than those pled in *Amnesty*. In the seven years since Section 702 took effect, and in the three years since the Supreme Court decided *Amnesty*, the public has gained a wealth of information about the government's implementation of its Section 702 authority, much of it formally confirmed in public, government-authorized disclosures. That information allows for the type of specific, plausible, non-speculative, and particularized claims of harm alleged by Plaintiffs here.

[4] And, even when the district court did acknowledge the claims of actual interception, the court simply discredited whether Upstream "*actually*" functions as plaintiffs alleged. *Wikimedia Found. v. National Security Agency/Central Security Service*, 2015 WL 6460364 at *10 (D. Md. Oct. 23, 2015) (emphasis in original). But in this respect, the district court failed to heed its own observation that it must "accept as true all material allegations of the complaint and construe the complaint in favor of the complaining party." *Id*. at *8. *See also Jewel v. NSA*, 673 F.3d at 907, 911 ("Jewel's complaint alleges past incidents of *actual* government interception of her electronic communications, a claim we accept as true.")

C. Plaintiffs' Plausible Allegations of Actual Interception of Internet Communications Provide the Requisite Injury in Fact for Standing Purposes, Just as They Did in *Jewel*.

The distinction between allegations of harm based on *possible*, future surveillance, and allegations of harm based on *actual* past and ongoing surveillance, serves as the dividing line for establishing standing. Where Plaintiffs plausibly allege that their communications were actually intercepted, they have Article III standing to challenge the surveillance.

The Ninth Circuit's decision in *Jewel*, 673 F.3d 902, confirms this dividing line. Filed in 2008, *Jewel* is a class action brought on behalf of AT&T customers that challenges the legality of various NSA surveillance programs directed at AT&T's communication platforms, including the NSA's Upstream surveillance of AT&T's Internet networks.[5] The core of the allegations in *Jewel* are based on eyewitness and documentary evidence of NSA surveillance equipment being installed at AT&T's facilities in San Francisco. *Jewel*, 673 F.3d at 910.

The Ninth Circuit found that these allegations were sufficient to establish a concrete, particularized, actual, and non-conjectural injury in fact. *Jewel*, 673 F.3d at 908 (citing *Lujan*, 504 U.S. at 560-61).[6]

---

[5] *Jewel* also includes statutory and constitutional claims based on the NSA's mass collection and search of domestic phone records. *See Jewel*, 673 F.3d at 906.

[6] Although *Jewel* was also initially dismissed on standing grounds, by contrast, there, the district court found that the alleged surveillance was so widespread and

That standard is met here, as it was in *Jewel*.

Just as in *Jewel*, Plaintiffs here allege past and ongoing incidents of actual government interception of their Internet communications. Their allegations are not based on how Section 702 *might* in the *future* be implemented. Rather, the detailed allegations are based on evidence—including government admissions—of past and ongoing interception of Internet communications. *See Jewel*, 673 F.3d at 910.

As in *Jewel*, the allegations of Plaintiffs "are highly specific and lay out concrete harms arising from the warrantless searches." *Id*. Namely, Plaintiffs allege concrete claims of violations of constitutional and statutory rights: *i.e*., that Upstream surveillance violates the First and Fourth Amendment rights of Plaintiffs; that the programmatic orders authorizing Upstream violate Article III of the Constitution; and that that Upstream surveillance exceeds the scope of the authority Congress provided in Section 702. *See* FAC ¶ 1; *Jewel,* 673 F.3d at 908–09.

And just as in *Jewel*, Plaintiffs' allegations of injury in this case are sufficiently particularized. The *Jewel* plaintiffs alleged with specificity a program of "dragnet" surveillance that "indiscriminately acquired domestic communications

---

the harms so widely shared that, in the court's view, it amounted to a "generalized grievance," unsuitable for resolution by the Article III courts. *Jewel*, 673 F.3d at 905, 906-07.

as well as international and foreign communications." *Jewel*, 673 F.3d at 910 (internal quotations omitted). Plaintiffs also allege with specificity that "the NSA is seizing Americans' communications en masse while they are in transit, and it is searching the contents of substantially all international text-based communications—and many domestic communications as well—for tens of thousands of search terms." FAC ¶ 1.

Critically, "Jewel alleged with particularity that *her* communications were part of the dragnet." 673 F.3d at 910. Plaintiffs also allege with particularity that their communications are caught up in the en masse seizure of Internet communications. *See, e.g.,* FAC ¶¶ 56-67. It is on this basis that the Ninth Circuit distinguished the allegations in *Jewel* from those in *Amnesty*:[7]

> Jewel has much stronger allegations of concrete and particularized injury than did the plaintiffs in *Amnesty* . . . Whereas they anticipated or projected future government conduct, Jewel's complaint alleges past incidents of *actual* government interception of her electronic communications, a claim we accept as true.

Jewel, 673 F.3d at 911 (emphasis in original).

The court in *Jewel* addressed an additional issue relevant here: the prudential considerations of national security litigation.

[7] The government had not yet petitioned for certiorari in *Amnesty* when *Jewel* was decided. Notably, the government did not seek Supreme Court review of the Ninth Circuit's decision in *Jewel*.

Although the *Amnesty* Court noted that the courts have sometimes declined to find standing in certain national security cases, *Amnesty*, 133 S. Ct. at 1147, national security does not bar consideration of cases where a concrete and particularized injury is present. *See Jewel*, 673 F.3d at 913 (discussing *Schlesinger v. Reservists Committee to Stop the War*, 418 U.S. 208 (1974)). As the Ninth Circuit recognized, although "prudential concerns may weigh against standing in certain cases affecting national security interests, . . . the national security context does not, in itself, erect a new or separate prudential bar to standing." 673 F.3d at 913. Even if national security concerns may pose "procedural, evidentiary and substantive barriers" to proving Plaintiffs' case, *Jewel*, 673 F.3d at 911, those concerns do not justify closing the courthouse door at the outset of a case.

II. OTHER AVENUES FOR OBTAINING JUDICIAL REVIEW OF UPSTREAM SURVEILLANCE HAVE PROVEN INSUFFICIENT.

Standing for civil litigants is particularly vital where there is a real risk of completely "immuniz[ing] Section 702 and Upstream surveillance from judicial scrutiny." *Wikimedia Found.,* 2015 WL 6460364 at *15. Both the Supreme Court in *Amnesty* and the district court below pointed to three avenues for legal review of Upstream surveillance that, in their view, ameliorated this concern: (1) FISC review of programmatic targeting and minimization procedures; (2) motions to suppress by defendants prosecuted

by evidence derived from Section 702 surveillance; and (3) challenges in the FISC by electronic communications service providers whose assistance in surveillance is compelled by 702 directives. *Id*.; *Amnesty*, 133 S. Ct. at 1154-55.

These avenues have failed to produce serious judicial scrutiny of Section 702, particularly for Upstream surveillance, underscoring the need for it in this case.

A. FISC Review of Upstream Surveillance Is an Inadequate Substitute for a Full and Adversarial Review of the Program.

The secret, *ex parte* proceedings of the FISC have not produced the fulsome legal review the Supreme Court anticipated when it decided *Amnesty*. The Court seemed to express confidence in the "comprehensive scheme" allowing for FISC review of Section 702 surveillance, including the FISC's review of "whether the targeting and minimization procedures comport with the Fourth Amendment." *Amnesty*, 133 S. Ct. at 1154. Yet, after nearly a decade of Upstream surveillance under Section 702, it does not appear that the FISC has ever considered—much less decided—the constitutional questions posed by Plaintiffs here.

Contrary to the district court's suggestion, there are no known FISC opinions that address the unique constitutional questions posed by this case.[8] The first FISC opinion to address Section 702 after the law's passage—an opinion described as the "Rosetta Stone" of Section 702 surveillance by executive branch officials[9]—fails to grapple seriously with the unique privacy issues presented by Upstream surveillance. In fact, in its discussion of the Fourth Amendment implications of Section 702 surveillance, the opinion fails to even mention Upstream surveillance or its critically distinguishing characteristics—namely, the wholesale interception and search of the *contents* of Internet communications. *See In re DNI/AG Certification* [Redacted], Dkt. No 702(i)-08-01, at 32-41 (FISC Sept. 4, 2008).[10] A second opinion, issued three years later, determined that the NSA's Upstream collection was unconstitutional. [*Redacted*], 2011 WL 10945618 (FISC Oct. 3, 2011). But even that opinion—which criticized the government for its

[8] The district court, in a footnote, suggested that "the FISC opinion that relates to the data collection practices challenged here is unavailable because it is classified." *Wikimedia Found.*, 2015 WL 6460364 at *5, n. 7. As described, *infra*, at least two FISC opinions have been released that consider Upstream surveillance. However, *amicus* is aware of no FISC opinion that addresses the unique legal questions posed by this case.

[9] *See Privacy and Civil Liberties Oversight Board Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* at 76 (Mar. 19, 2014) (statement of James Dempsey, Board Member, Privacy and Civil Liberties Oversight Board), *available at* https://www.pclob.gov/library/20140319-Transcript.pdf.

[10] *Available at* http://www.dni.gov/files/documents/0315/FISC%20Opinion%20September%204%202008.pdf.

repeated "substantial misrepresentation[s]," *id.* at *5, n.14—did not confront the basic constitutional question presented by Plaintiffs in this case. In sum, it does not appear that the FISC has ever considered the constitutional implications raised by surveillance that sifts through vast quantities of Americans' Internet communications.

This is so for a single reason: the secret, *ex parte* nature of proceedings before the FISC. As the Supreme Court noted, "fairness can rarely be obtained by secret, one-sided determination[s]." *Joint Anti-Fascist Refugee Comm. v. McGrath*, 341 U.S. 123, 170 (1951) (Frankfurter, J., concurring). Rather, our adversarial system "is premised on the well-tested principle that truth—as well as fairness—is best discovered by powerful statements on both sides of the question." *Penson v. Ohio*, 488 U.S. 75, 84, (1988) (internal quotations omitted). *Ex parte* proceedings, like those in the FISC, are especially avoided because of the unacceptable risk of error. *See Lynn v. Regents of Univ. of California*, 656 F.2d 1337, 1346 (9th Cir. 1981) ("The system functions properly and leads to fair and accurate resolutions, only when vigorous and informed argument is possible.").

Those risks have borne out in the FISC's decisions. The FISC's treatment of the NSA's phone records bulk collection program and the Court's interpretation of Section 215 of the USA PATRIOT Act, Pub. Law No. 107-56, 115 Stat. 272 (Oct. 26, 2001), are instructive. The FISC did not undertake a 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]*, Dkt. No. BR 13-109 (FISC Aug. 29, 2013),[11] *with In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted]*, Dkt. No. BR 06-05 (FISC May 24, 2006).[12] Yet, in little more than two years of public, adversarial testing of the phone records program, two federal courts found the NSA's program to be 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 and remanded*, 800 F.3d 559 (D.C. Cir. 2015).

The shortcomings in the FISC's *ex parte* process are exacerbated by two facts.

First, the FISA Amendments Act transformed the FISC "into a 'meta-arbiter,' approving generally applicable targeting and minimization procedures. . . . [P]rior to 2008, FISA required FISC to approve individualized warrant applications *before* a given search occurred, consistent with the recommendations of the Church Committee." Walter F. Mondale, Robert A. Stein, Caitlinrose Fisher, *No Longer a Neutral Magistrate: The Foreign Intelligence Surveillance Court in the Wake of*

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

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

the War on Terror, Minn. L. Rev., forthcoming, 14, 20 (Jan. 1, 2016) (emphasis in original) ("*No Longer a Neutral Magistrate*").[13] As explained in this forthcoming law review article, co-authored by former-Vice President Mondale (an influential member of the Church Committee), since enactment of the FAA, the FISC has applied "general and ambiguous language to (almost always) give judicial credence to intelligence agency procedures, in the absence of specific information about the search targets." *Id.* at 22. As the FISC itself has acknowledged, its review of the government's practices under Section 702 "is limited." *In re DNI/AG Certification* [*Redacted*], Dkt. No. 702(i)-08-01 (FISC Sept. 4, 2008). This limited review has transformed the FISC into "more of a rubber stamp on behalf of the government than a neutral check against executive overreach." *No Longer a Neutral Magistrate* at 34.

Second, the government has repeatedly failed to provide the FISC with accurate and comprehensive information regarding the legal and factual questions before it. Again, using the NSA's phone records program as an example, it took the FISC two years after the issuance of its initial order authorizing the bulk collection of domestic phone records to assess the significance of another statute, the Stored Communications Act, 18 U.S.C. § 2700, *et seq*. ("SCA"), that specifically governs the disclosure of call records from telecommunications providers. *See In re*

[13] *Available at* http://ssrn.com/abstract=2712892.

Production of Tangible Things from [*Redacted*], Dkt. No. BR 08-13 (FISC Dec. 12, 2008).[14] The SCA was plainly necessary for the FISC's consideration of the program and its interpretation of Section 215 in the first instance, but it was not brought to the court's attention until nearly two years after the program began.

The government likewise has a checkered history of providing accurate factual information to the court. As Judge Reggie Walton, the former presiding judge of the FISC, noted: "The FISC is forced to rely upon the accuracy of the information provided to the Court." Carol Leonnig, *Court: Ability to Police U.S. Spying Program Limited*, Wash. Post (Aug. 15, 2013).[15] And the reliability of the information provided has repeatedly proven suspect. A FISC decision, issued by Judge John Bates in 2011, lamented 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." [*Redacted*], 2011 WL 10945618 at * 5 n. 14; *see also*, *In re Production of Tangible Things from [Redacted]*, Dkt. No. BR 08-13 at 14 (FISC Mar. 2, 2009) (describing government's "historical record of non-compliance" with FISC's orders).[16] With a limited review, one-sided legal briefing,

[14] *Available at* https://www.aclu.org/files/assets/pub_Dec%2012%202008%20Supplemental%20Opinions%20from%20the%20FISC.pdf.
[15] *Available at* https://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_story.html.
[16] *Available at* https://www.eff.org/files/filenode/br_08-13_order_3-2-09_final_redacted.ex_-_ocr_1.pdf.

and incomplete factual disclosures, the FISC's review of Section 702 is necessarily incomplete.

B. Criminal Defendants Have Been Unable to Challenge Upstream Surveillance.

Even criminal defendants whose prosecutions are based on evidence derived from Upstream surveillance are functionally barred from challenging this surveillance.

First, until October 2013, defendants who were subject to *any* form of Section 702 surveillance (PRISM or Upstream) were simply unaware of this fact. In its briefs and at oral argument in *Amnesty*, the government assured the Supreme Court that "aggrieved persons" subject to surveillance would receive notice that the government "intend[ed] to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding . . . any information obtained or derived from an electronic surveillance." 50 U.S.C. § 1806(c); *see* Br. for Petitioner, *Amnesty*, 2012 WL 3090949 at *8; Tr. of Oral Argument at 2-4.[17]

Those representations were false.

Instead, the Justice Department "had not been alerting such defendants that evidence in their cases had stemmed from wiretapping their conversations without

[17] *Available at* http://www.supremecourt.gov/oral_arguments/argument_transcripts/11-1025.pdf.

a warrant."[18] 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.* These disclosures showed "that the administration deliberately masked evidentiary trails to hide any evidence that originated from" FISA surveillance so that the surveillance "could not be challenged in criminal proceedings."[19]

The government has now notified a handful of "Clapper-qualified" defendants whose prosecutions involve evidence derived from Section 702 surveillance. *United States v. Muhtorov*, No. 12-CR-33, Slip Op. at 2 (D. Colo. Nov. 19, 2015).[20] However, *amicus* is aware of only five cases in which the government has belatedly provided such "supplemental" FISA notifications, in some cases *after* sentencing. *See id.* ("[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[.]"); *United States v. Mohamud*, No. 10-CR-00475, 2014 WL

[18] Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. Times (Oct. 16, 2013), *available at* http://www.nytimes.com/2013/10/17/us/politics/us-legal-shift-may-open-door-for-challenge-to-secret-wiretaps.html.
[19] *No Longer a Neutral Magistrate* at 26 (citing John Shiffman & Kristina Cooke, *U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, REUTERS (Aug. 5, 2013), *available at* http://www.reuters.com/article/us-deasod-idUSBRE97409R20130805).
[20] *Available at* https://www.justsecurity.org/wp-content/uploads/2015/11/5271610-0-11699.pdf.

2866749 (D. Or. June 24, 2014), *appeal docketed* No. 14-30217; *Hasbajrami v. United States*, No. 11-CR-623 (E.D.N.Y. 2015), *appeal docketed* No. 15-2684; *United States v. Khan*, No. 12-CR-00659, (D. Or. 2014) (ECF No. 59) (supplemental notice of Section 702 surveillance);[21] *United States v. Mihalik,* No. 11-CR-833 (C.D. Cal. 2014) (ECF No. 145) (supplemental notice of Section 702 surveillance).[22]

These five cases are dwarfed by the number of individuals targeted for surveillance under Section 702. According to the latest transparency report released by the ODNI, there were a 92,707 "targets" affected by a *single* FISC 702 certification in 2014. Office of the Director of National Intelligence, *Calendar Year 2014 Transparency Report*, IC on the Record (April 22, 2015).[23] But due to the programmatic nature of Section 702 surveillance, the number of targets is itself far outnumbered by the individuals whose communications are "incidentally" acquired.[24] Unless a larger number of these individuals are prosecuted for crimes

[21] *Available at* https://ia801703.us.archive.org/35/items/gov.uscourts.ord.110335/gov.uscourts.ord.110335.59.0.pdf.
[22] *Available at* https://ia902606.us.archive.org/2/items/gov.uscourts.cacd.511083/gov.uscourts.cacd.511083.145.0.pdf
[23] *Available at* http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.
[24] *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), *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*

discovered through this surveillance, and unless the government unilaterally determines they qualify as "aggrieved persons" under FISA, challenges to Section 702 arising in the criminal context will remain exceedingly rare. *See United States v. U.S. Dist. Court for E. Dist. of Mich.*, 407 U.S. 297, 318 (1972) (individualized prior review by neutral and detached magistrate required because "post-surveillance review would never reach the surveillances which failed to result in prosecutions").

Even where criminal defendants do receive notice and thus have undisputed standing to challenge Section 702 surveillance, they have been barred from accessing the information necessary to make such a challenge. Crucially, the notifications provided to date by the government do not specify *which* Section 702 program was used to acquire the defendants' communications, or even which of their communications were actually acquired. Thus, the supplemental notifications in these cases do not answer the threshold question of whether the case implicates Upstream surveillance at all, or instead involves some other program authorized under Section 702, such as PRISM. And the government has so far refused to provide defendants with this information through discovery. *See Mohamud*, 2014

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.

WL 2866749 at *32 (denying motion for discovery into which program the government used to surveil defendants as not "necessary" for "an accurate determination of the legality of the surveillance" under 50 U.S.C. § 1806(f)).[25]

Because they do not know whether the government acquired their communications using Upstream versus PRISM, criminal defendants are hamstrung in their challenges to Section 702. Instead, they are left with arguments that are far less concrete than Plaintiffs' arguments here. In *Muhtorov,* for example, the court summarily rejected the defendant's argument that Section 702 involves a "vacuum-cleaner-style mass collection of virtually every person's international communications" as overly "generalized." *Muhtorov*, No. 12-CR-33, Slip Op. at 29. By contrast, the complaint in this case involves detailed allegations regarding the interception of Plaintiffs' communications specific to the government's Upstream program. *See* FAC ¶¶ 47-51. Without similar specific factual grounding, criminal defendants are prevented from robust challenges to Upstream surveillance.

[25] *See also* Faiza Patel, *How a Case of Stolen Corn Seeds Shows the Problem with the FISA Court*, JUST SECURITY (Apr. 1, 2015) (noting how the government notice of FISA-collected evidence often does not include the basis of collection—who was the "foreign agent," what statutory provision the search was authorized under—leaving defense counsel unable to effectively bring a motion to suppress the evidence), *available at* https://www.justsecurity.org/21709/stolen-corn-seeds-problem-fisa-court/.

C. Challenges by Service Providers Have Proven To Be an Unrealistic Avenue for Obtaining Legal Review of Upstream Surveillance.

The third avenue for review of Upstream surveillance identified by the *Amnesty* Court was an "electronic communications service provider that the Government directs to assist" in Upstream surveillance. But to date, no provider has challenged the legality of this surveillance, nor is such a challenge likely.[26]

The service providers that operate the nation's fiber-optic network backbone—like AT&T and Verizon—are the same companies that participated in warrantless NSA surveillance, known as the President's Surveillance Program, conducted solely under presidential authority from 2001 to 2006; that turned over call records of its customers in bulk from 2006 to 2015; and that have participated in Upstream surveillance under the FAA since 2008. *See* Julia Angwin, *et al*., *A Trail of Evidence Leading to AT&T's Partnership with the NSA*, ProPublica (Aug. 15, 2015).[27] *See also* Office of the Inspector General of the NSA/CSS, *Working Draft Report* at 28-34 (Mar. 24, 2009) (describing "partnerships" with companies

[26] In 2007, Yahoo! challenged the constitutionality of orders it had received under the Protect America Act, the predecessor to the FISA Amendments Act. *See In re Directives* [*Redacted*] *Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004 (FISCR 2008). But the role—and the resistance—of Internet platform companies like Yahoo! to participating in legally questionable surveillance stands in stark contrast to the lengthy and unquestioning relationship operators of the nation's fiber optic backbone—like AT&T and Verizon—have enjoyed with the NSA, as described *infra*.

[27] *Available at* https://www.propublica.org/article/a-trail-of-evidence-leading-to-atts-partnership-with-the-nsa.

in President's surveillance program and call records program).[28] Despite the tenuous legal foundation of these surveillance programs, *none* spurred a challenge to the legality of the collection from a major provider.

And there is no reason to believe they will in the future, because there is little financial incentive for the companies to do so. Records reveal that government surveillance constitutes a significant revenue stream for these companies. Julia Angwin, *et al., NSA Spying Relies on AT&T's 'Extreme Willingness to Help,'* ProPublica (Aug. 15, 2015) (describing NSA expenditures of $188.9 million on AT&T surveillance program).[29] The NSA views its relationship with these companies as "highly collaborative," more reminiscent of a partnership than a likely candidate for adversarial litigation. For the nation's largest telecommunication companies, there is little financial risk posed by these "collaborative" relationships, either. The FAA provided broad immunity from suit for their assistance with national security surveillance. *See In re NSA Telecommunications Records Litigation*, 671 F.3d 881 (9th Cir. 2011) (finding Section 802 of FISA, codified by the FAA at 50 U.S.C. § 1885a, immunized AT&T from suit for its participation in the national security surveillance program).

[28] *Available at* http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection.
[29] *Available at* https://www.propublica.org/article/nsa-spying-relies-on-atts-extreme-willingness-to-help.

From the perspective of the nation's largest telecommunication providers, more government surveillance simply means more government money. The operators of the nation's fiber optic backbone have found little financial incentive to deviate from that course. [30]

[30] The district court suggested one additional avenue for legal review of Upstream surveillance:

> Should society's suspicions about surveillance programs rise to a level sufficient to cause citizens to suspect Orwellian harms that outweigh the benefits to national security, surveillance programs can be revised or eliminated the same way they were authorized, namely through the legislative process.

Wikimedia Found., 2015 WL 6460364 at *15, n. 28.

First, this observation incorrectly assumes that the legislative process that led to the passage of Section 702 was transparent and marked by the robust democratic debate the district court idealizes. It was not. In fact, the government did not publicly acknowledge it conducted Upstream surveillance until 2013—*five years* after Section 702 was first passed. *See* Office of the Director of National Intelligence, *DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702 of the Foreign Intelligence Surveillance Act (FISA)*, IC on the Record (Aug. 21, 2013), *available at* http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents.

Second, reliance on such an approach abdicates the judiciary's "unflagging" obligation to "hear and decide cases within its jurisdiction." *Lexmark*, 134 S. Ct. at 1386. Although there can be "little doubt that [Plaintiffs' case] challenges conduct that strikes at the heart of a major public controversy involving national security and surveillance" and that "the claims arise from political conduct and in a context that has been highly politicized," this case raises "straightforward claims of statutory and constitutional rights, not political questions." *See Jewel*, 673 F.3d at 912. Thus, the judiciary can and should decide this matter.

CONCLUSION

For the foregoing reasons, this Court should reverse the district court's order.

Dated: February 24, 2016

Respectfully submitted,

/s/ Sophia Cope

Sophia Cope
Mark Rumold
Andrew Crocker
Jaime Williams
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Counsel for Amicus Curiae Electronic Frontier Foundation

CERTIFICATE OF COMPLIANCE
WITH TYPE-VOLUME LIMITATION,
TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS
PURSUANT TO FED. R. APP. P. 32(A)(7)(C)

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of Amicus Curiae in Support of Appellant complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 5,592 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); 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 2011, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: February 24, 2016

/s/ Sophia Cope
Sophia Cope

Counsel for Amicus Curiae
Electronic Frontier Foundation

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 February 24, 2016.

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: February 24, 2016

/s/ Sophia Cope
Sophia Cope

Counsel for Amicus Curiae
Electronic Frontier Foundation

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

APPEARANCE OF COUNSEL FORM

BAR ADMISSION & ECF REGISTRATION: If you have not been admitted to practice before the Fourth Circuit, you must complete and return an Application for Admission before filing this form. If you were admitted to practice under a different name than you are now using, you must include your former name when completing this form so that we can locate you on the attorney roll. Electronic filing by counsel is required in all Fourth Circuit cases. If you have not registered as a Fourth Circuit ECF Filer, please complete the required steps at Register for eFiling.

THE CLERK WILL ENTER MY APPEARANCE IN APPEAL NO. 15-2560 as

☐ Retained ☐ Court-appointed(CJA) ☐ Court-assigned(non-CJA) ☐ Federal Defender ☑ Pro Bono ☐ Government

COUNSEL FOR: Electronic Frontier Foundation

_____ as the
(party name)

☐ appellant(s) ☐ appellee(s) ☐ petitioner(s) ☐ respondent(s) ☑ amicus curiae ☐ intervenor(s) ☐ movant(s)

/s/ Sophia Cope
(signature)

Sophia Cope
Name (printed or typed)

415-436-9333
Voice Phone

Electronic Frontier Foundation
Firm Name (if applicable)

415-436-9993
Fax Number

815 Eddy Street

San Francisco, CA 94109
Address

sophia@eff.org
E-mail address (print or type)

CERTIFICATE OF SERVICE

I certify that on 2/24/2016 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

/s/ Sophia Cope
Signature

2/24/2016
Date