**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | |
|---|---|
| WIKIMEDIA FOUNDATION, *et al.*, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants. | Civil Action No. 1:15-cv-00662-TSE |

**MEMORANDUM IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS THE FIRST AMENDED COMPLAINT**

Date: August 6, 2015

BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Deputy Branch Director

JAMES J. GILLIGAN
Special Litigation Counsel

RODNEY PATTON
JULIA A. BERMAN
CAROLINE J. ANDERSON
Trial Attorneys

U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 6102
Washington, D.C. 20044
Phone: (202) 514-3358
Fax: (202) 616-8470
E-mail: james.gilligan@usdoj.gov

Counsel for Defendants

**TABLE OF CONTENTS**

**PAGE**

INTRODUCTION ..... 1

BACKGROUND ..... 4

The Foreign Intelligence Surveillance Act ..... 4

The FISA Amendments Act of 2008 ..... 6

Upstream Collection Under Section 702 ..... 9

Plaintiffs' Allegations ..... 10

ARGUMENT ..... 14

I. LEGAL STANDARDS ..... 14

A. Pleading Standards Under *Twombly* and *Iqbal* ..... 14

B. The Requirements of Standing ..... 14

II. PLAINTIFFS HAVE NOT PLAUSIBLY ALLEGED THAT THEY HAVE BEEN INJURED BY THE INTERCEPTION, COPYING, AND REVIEW OF THEIR ONLINE COMMUNICATIONS IN THE UPSTREAM COLLECTION PROCESS ..... 16

A. Plaintiffs Have Not Plausibly Alleged That Upstream Collection Involves the Interception, Copying, and Selector Review of Substantially All International Online Communications Transiting the United States ..... 16

B. Neither the Alleged "Extraordinarily High Volume" and Global Distribution of Wikimedia's Communications, Nor Plaintiffs' Unilateral Assumptions About How Upstream Surveillance "Must Be" Conducted to Achieve Its Objectives, Establishes That Any of the Plaintiffs' Communications (Including Wikimedia's) Are Intercepted, Copied, or Reviewed for Selectors in the Upstream Collection Process ..... 20

1. Wikimedia's Co-Plaintiffs Cannot Base Their Standing on the Alleged Number and Distribution of Visits to Wikimedia Websites ..... 21

**PAGE**

2. Wikimedia's Alleged International Online Communications Represent Only a Small Proportion of the Total Volume of Communications Carried on the Internet....24

3. Wikimedia's Allegation That the Volume of its Communications Makes Interception of at Least Some of Those Communications a Virtual Certainty is Statistically Unsupported....27

4. Wikimedia's Allegation That the Geographic Distribution of its Communications Makes Interception of Those Communications a Virtual Certainty Also Rests on Unsupported Speculation About the Manner in Which Upstream Surveillance is Conducted....29

5. The Allegation that the Volume and Distribution of Wikimedia's Communications Make it Likely That They Have Been Intercepted, Copied, and Reviewed in the Upstream Process is Legally Insufficient, Under *Amnesty International*, to Establish Wikimedia's Standing....32

C. Wikimedia Has Alleged No Injury from the Claimed Interception, Copying and Review of Its Online Communications....34

III. PLAINTIFFS HAVE NOT PLAUSIBLY ALLEGED THAT COMMUNICATIONS OF THEIRS ARE RETAINED, READ, AND DISSEMINATED BY THE NSA AS PART OF THE UPSTREAM SURVEILLANCE PROCESS....40

A. Plaintiffs' Allegations That Their Staffs Engage in Communications With Likely Targets of Upstream Surveillance, About Topics That Could Be Considered Foreign-Intelligence Information, Are Insufficient Under *Amnesty International* to Establish Their Standing....40

B. NACDL Has Not Established Its Standing to Sue on Behalf of its Members....42

IV. PLAINTIFFS' ALLEGATIONS THAT UPSTREAM COLLECTION "UNDERMINES [THEIR] ABILITY TO CONDUCT [THEIR] WORK" ALSO FAIL TO ESTABLISH AN INJURY SUFFICIENT TO CONFER STANDING....47

CONCLUSION....50

## TABLE OF AUTHORITIES

**CASES** **PAGE(S)**

*American Immigration Lawyers Ass'n v. Reno*,
199 F.3d 1352 (D.C. Cir. 2000) ..... 39

*Amnesty Int'l USA v. Clapper*,
638 F.3d 118 (2d Cir. 2011), *rev'd*, 133 S. Ct. 1138 (2013) ..... 11

*Ashcroft v. Iqbal*,
556 U.S. 662 (2009) ..... *passim*

*Bell Atlantic Corp. v. Twombly*,
550 U.S. 544 (2007) ..... *passim*

*Blum v. Yaretsky*,
457 U.S. 991 (1982) ..... 23

*Burke v. City of Charleston*,
139 F.3d 401 (4th Cir. 1998) ..... 14, 15

*California Bankers Ass'n v. Schultz*,
416 U.S. 21 (1974) ..... 39

[*Caption Redacted*],
2011 WL 10945618 (F.I.S.C. Oct. 3, 2011) ..... 19, 45

[*Caption Redacted*],
2011 WL 10947772 (F.I.S.C. Nov. 30, 2011) ..... 19

*Carey v. Population Servs. Int'l* ,
431 U.S. 678 (1979) ..... 39

*Clapper v. Amnesty Int'l, USA*,
133 S. Ct. 1138 (2013) ..... *passim*

*David v. Alphin*,
704 F.3d 327 (4th Cir. 2013) ..... 14, 34

*Doe v. Va. Dept. of St. Police*,
713 F.3d 745 (4th Cir. 2013) ..... 15, 16, 37

*Fenstermaker v. Bush*,
2007 WL 1705068 (S.D.N.Y. June 12, 2007) ..... 39

**PAGE(S)**

*Freilich v. Upper Chesapeake Health, Inc.*,
313 F.3d 205 (4th Cir. 2002) ..... 15, 38

*Friends of the Earth, Inc. v. Laidlaw Envt'l Servs.*,
528 U.S. 167 (2000) ..... 23

*Jewel v. NSA*,
2015 WL 545925 (N.D. Cal. Feb. 10, 2015) ..... 4, 32, 40

*Katz v. United States*,
389 U.S. 347 (1967) ..... 36

*Kowalski v. Tesmer*,
543 U.S. 125 (2004) ..... 15, 37, 38

*Laird v. Tatum*,
408 US. 1 (1972) ..... 50

*Lewis v. Casey*,
518 U.S. 343 (1996) ..... 23

*Lujan v. Defenders of Wildlife*,
504 U.S. 555 (1992) ..... 15, 23

*Maryland v. Macon*,
472 U.S. 463 (1985) ..... 36

*Miller v. Albright*,
523 U.S. 420, 449 (1998) ..... 40

*Murphy-Taylor v. Hofmann*,
968 F. Supp. 2d 693 (D. Md. 2013) ..... 19

*Rakas v. Illinois*,
439 U.S. 128 (1978) ..... 39

*In re Motion for Release of Court Records*,
526 F. Supp. 2d 484 (F.I.S.C. 2007) ..... 5

*Shenandoah Valley Network v. Capka*,
669 F.3d 194 (4th Cir. 2012) ..... 15

*Simon v. E. Ky. Welfare Rights Org.*,
426 U.S. 26 (1976) ..... 23

**PAGE(S)**

*Singleton v. Wulff*,
428 U.S. 106 (1976) ..... 39

*Southern Walk at Broadlands Homeowner's Ass'n, Inc. v. OpenBand at Broadlands, LLC*, 713 F.3d 175 (4th Cir. 2013) ..... 20, 43

*Stephens v. City of Albermarle, Virginia*,
524 F.3d 485 (4th Cir. 2008) ..... 15, 17

*Summers v. Earth Island, Inst.*,
555 U.S. 488 (2009) ..... *passim*

*United Food & Commercial Workers Union Local 751 v. Brown Group, Inc.*,
517 U.S. 544 (1996) ..... 43

*United States v. Baalerud*,
2015 WL 1349821 (W.D.N.C. Mar. 25, 2015) ..... 36

*United States v. Hasbajrami*,
1:11-cr-00623 (E.D.NY.), ECF No. 65 (Feb. 24, 2014) ..... 46

*United States v. Moalin*, ,
2013 WL 6079518 (S.D. Cal. Nov. 18, 2013) ..... 47

*Unites States v. Mohamud*,
2014 WL 2866749 (June 24, 2014) ..... 39, 46

*United States v. Verdugo-Urquidez*,
494 U.S. 259 (1990) ..... 39

*United States ex rel. Oberg v. Pennsylvania Higher Educ. Assistance Agency*,
745 F.3d 131 (4th Cir. 2014) ..... 18

*Valley Forge Christian Coll. v. Americans United for Separation of Church & State, Inc.*, 454 U.S. 464 (1982) ..... 14, 16, 22

*Velasco v. Gov't of Indonesia*,
370 F.3d 392 (4th Cir.2004) ..... 19

*Vitol, S.A. v. Primerose Shipping Co.*,
708 F.3d 527 (4th Cir. 2013) ..... 14

**PAGE(S)**

*Warth v. Seldin*,
422 U.S. 490 (1975) ..... 15, 16

*Zander v. United States*,
786 F. Supp. 2d 880 (D. Md. 2011) ..... 14, 34

**STATUTES**

50 U.S.C. § 1801 ..... *passim*

50 U.S.C. § 1803 ..... 5

50 U.S.C. § 1804 ..... 5

50 U.S.C. § 1805 ..... 5

50 U.S.C. § 1881a ..... 7, 8, 9, 41

The FISA Amendments Act of 2008 ("FAA"),
Pub. L. No. 110-261 (2008) ..... *passim*

**LEGISLATIVE MATERIALS**

Executive Order 12333, 46 Fed. Reg. 59941 (Dec. 4, 1981),
*reprinted as amended*, 50 U.S.C. § 3001 ..... 6, 42

H.R. Rep. No. 645(II), 112th Cong., 2d Sess. (2012) ..... 10

H.R. Rep. No. 95-1283(I), 95th Cong., 2d Sess. (1978) ..... 6

*Modernization of the FISA: Hearing before the S. Select Comm. on Intel.*,
110th Cong., 1st Sess. (2007) ..... 6, 7

S. Rep. No. 110-209 (2007) ..... 6

S. Rep. No. 209, 110th Cong., 1st Sess. (2007) ..... 6

S. Rep. No. 174, 112th Cong., 2d Sess. (2012) ..... 10

S. Rep. No. 604, 95th Cong., 1st Sess. (1977) ..... 4, 5

S. Rep. No. 701, 95th Cong., 2d Sess. (1978) ..... 5, 6

## INTRODUCTION

One of the greatest challenges the United States faces in combating international terrorism and other potentially catastrophic threats to the safety and welfare of our Nation is identifying terrorist operatives and networks, and other foreign dangers. The Government's exploitation of our foreign enemies' communications is a critical tool in this effort. Plaintiffs in this case ask the Court to invalidate and enjoin a uniquely valuable means by which the National Security Agency ("NSA"), acting under the authority and oversight of the Foreign Intelligence Surveillance Court ("FISC"), gathers communications by and among our foreign adversaries in order to detect and thwart peril to our Nation and its people.

Plaintiffs seek to contest the legality of NSA "Upstream" surveillance, a program under which the NSA targets certain non-U.S. persons reasonably believed to be located outside the United States in order to acquire foreign-intelligence information. The NSA targets these individuals by acquiring online communications as they transit the Internet "backbone" networks of U.S. telecommunications service providers. Upstream surveillance is conducted under authority of Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), pursuant to targeting and minimization procedures (procedures to minimize the acquisition, retention, and dissemination of U.S.-person information) that must be approved by the FISC as consistent with statutory requirements and the Constitution. Upstream's unique capabilities and contributions to national security have been recognized by all three branches of the Federal Government. Plaintiffs nevertheless maintain that Upstream collection exceeds the Government's authority under Section 702, violates the Constitution, and should be permanently enjoined. These claims should be dismissed, because Plaintiffs have not established their standing to assert them.

Although the technical operational details of Upstream surveillance remain classified, Plaintiffs hypothesize that it involves an initial stage at which the NSA intercepts, copies, and

## TABLE OF AUTHORITIES

**CASES** **PAGE(S)**

*American Immigration Lawyers Ass'n v. Reno*,
199 F.3d 1352 (D.C. Cir. 2000) ..... 39

*Amnesty Int'l USA v. Clapper*,
638 F.3d 118 (2d Cir. 2011), *rev'd*, 133 S. Ct. 1138 (2013) ..... 11

*Ashcroft v. Iqbal*,
556 U.S. 662 (2009) ..... *passim*

*Bell Atlantic Corp. v. Twombly*,
550 U.S. 544 (2007) ..... *passim*

*Blum v. Yaretsky*,
457 U.S. 991 (1982) ..... 23

*Burke v. City of Charleston*,
139 F.3d 401 (4th Cir. 1998) ..... 14, 15

*California Bankers Ass'n v. Schultz*,
416 U.S. 21 (1974) ..... 39

[*Caption Redacted*],
2011 WL 10945618 (F.I.S.C. Oct. 3, 2011) ..... 19, 45

[*Caption Redacted*],
2011 WL 10947772 (F.I.S.C. Nov. 30, 2011) ..... 19

*Carey v. Population Servs. Int'l* ,
431 U.S. 678 (1979) ..... 39

*Clapper v. Amnesty Int'l, USA*,
133 S. Ct. 1138 (2013) ..... *passim*

*David v. Alphin*,
704 F.3d 327 (4th Cir. 2013) ..... 14, 34

*Doe v. Va. Dept. of St. Police*,
713 F.3d 745 (4th Cir. 2013) ..... 15, 16, 37

*Fenstermaker v. Bush*,
2007 WL 1705068 (S.D.N.Y. June 12, 2007) ..... 39

**PAGE(S)**

*Freilich v. Upper Chesapeake Health, Inc.*,
313 F.3d 205 (4th Cir. 2002) ..... 15, 38

*Friends of the Earth, Inc. v. Laidlaw Envt'l Servs.*,
528 U.S. 167 (2000)..... 23

*Jewel v. NSA*,
2015 WL 545925 (N.D. Cal. Feb. 10, 2015) ..... 4, 32, 40

*Katz v. United States*,
389 U.S. 347 (1967)..... 36

*Kowalski v. Tesmer*,
543 U.S. 125 (2004)..... 15, 37, 38

*Laird v. Tatum*,
408 US. 1 (1972)..... 50

*Lewis v. Casey*,
518 U.S. 343 (1996)..... 23

*Lujan v. Defenders of Wildlife*,
504 U.S. 555 (1992)..... 15, 23

*Maryland v. Macon*,
472 U.S. 463 (1985)..... 36

*Miller v. Albright*,
523 U.S. 420, 449 (1998)..... 40

*Murphy-Taylor v. Hofmann*,
968 F. Supp. 2d 693 (D. Md. 2013)..... 19

*Rakas v. Illinois*,
439 U.S. 128 (1978)..... 39

*In re Motion for Release of Court Records*,
526 F. Supp. 2d 484 (F.I.S.C. 2007)..... 5

*Shenandoah Valley Network v. Capka*,
669 F.3d 194 (4th Cir. 2012) ..... 15

*Simon v. E. Ky. Welfare Rights Org.*,
426 U.S. 26 (1976)..... 23

**PAGE(S)**

*Singleton v. Wulff*,
428 U.S. 106 (1976) ..... 39

*Southern Walk at Broadlands Homeowner's Ass'n, Inc. v. OpenBand at Broadlands, LLC*, 713 F.3d 175 (4th Cir. 2013) ..... 20, 43

*Stephens v. City of Albermarle, Virginia*,
524 F.3d 485 (4th Cir. 2008) ..... 15, 17

*Summers v. Earth Island, Inst.*,
555 U.S. 488 (2009) ..... *passim*

*United Food & Commercial Workers Union Local 751 v. Brown Group, Inc.*,
517 U.S. 544 (1996) ..... 43

*United States v. Baalerud*,
2015 WL 1349821 (W.D.N.C. Mar. 25, 2015) ..... 36

*United States v. Hasbajrami*,
1:11-cr-00623 (E.D.NY.), ECF No. 65 (Feb. 24, 2014) ..... 46

*United States v. Moalin*, ,
2013 WL 6079518 (S.D. Cal. Nov. 18, 2013) ..... 47

*Unites States v. Mohamud*,
2014 WL 2866749 (June 24, 2014) ..... 39, 46

*United States v. Verdugo-Urquidez*,
494 U.S. 259 (1990) ..... 39

*United States ex rel. Oberg v. Pennsylvania Higher Educ. Assistance Agency*,
745 F.3d 131 (4th Cir. 2014) ..... 18

*Valley Forge Christian Coll. v. Americans United for Separation of Church & State, Inc.*, 454 U.S. 464 (1982) ..... 14, 16, 22

*Velasco v. Gov't of Indonesia*,
370 F.3d 392 (4th Cir.2004) ..... 19

*Vitol, S.A. v. Primerose Shipping Co.*,
708 F.3d 527 (4th Cir. 2013) ..... 14

**PAGE(S)**

*Warth v. Seldin*,
422 U.S. 490 (1975) ..... 15, 16

*Zander v. United States*,
786 F. Supp. 2d 880 (D. Md. 2011) ..... 14, 34

**STATUTES**

50 U.S.C. § 1801 ..... *passim*

50 U.S.C. § 1803 ..... 5

50 U.S.C. § 1804 ..... 5

50 U.S.C. § 1805 ..... 5

50 U.S.C. § 1881a ..... 7, 8, 9, 41

The FISA Amendments Act of 2008 ("FAA"),
Pub. L. No. 110-261 (2008) ..... *passim*

**LEGISLATIVE MATERIALS**

Executive Order 12333, 46 Fed. Reg. 59941 (Dec. 4, 1981),
*reprinted as amended*, 50 U.S.C. § 3001 ..... 6, 42

H.R. Rep. No. 645(II), 112th Cong., 2d Sess. (2012) ..... 10

H.R. Rep. No. 95-1283(I), 95th Cong., 2d Sess. (1978) ..... 6

*Modernization of the FISA: Hearing before the S. Select Comm. on Intel.*,
110th Cong., 1st Sess. (2007) ..... 6, 7

S. Rep. No. 110-209 (2007) ..... 6

S. Rep. No. 209, 110th Cong., 1st Sess. (2007) ..... 6

S. Rep. No. 174, 112th Cong., 2d Sess. (2012) ..... 10

S. Rep. No. 604, 95th Cong., 1st Sess. (1977) ..... 4, 5

S. Rep. No. 701, 95th Cong., 2d Sess. (1978) ..... 5, 6

reviews substantially all international online communications—including theirs—as they transit U.S. telecommunications networks, to identify communications containing selectors associated with the NSA's surveillance targets. Plaintiffs allege that targeted communications, once identified, are retained in Government databases for analysis and dissemination of any foreign-intelligence information they contain. They allege further that communications of theirs are substantially likely to be among those retained, read, and disseminated by the NSA. Plaintiffs maintain that Upstream surveillance invades their interest in the privacy of their online communications and violates their right to control the information they contain.

This case does not mark the first occasion on which litigants have sought to challenge alleged NSA surveillance activities conducted under Section 702. In *Clapper v. Amnesty Int'l, USA*, 133 S. Ct. 1138 (2013), various human rights, labor, and media organizations—six of which are also plaintiffs in this case—sought to mount a facial constitutional challenge to Section 702. They alleged that communications of theirs would likely be subject to Government surveillance, because they interacted and communicated with persons who were probable targets of surveillance under Section 702. *Id.* at 1145–46. The Supreme Court held, however, that these allegations were insufficient to confer standing, because it was "speculative whether the Government [would] imminently target communications to which [the plaintiffs] [we]re parties." *Id.* at 1148. Rather, the Court held that the plaintiffs' harm rested on a "speculative chain of possibilities," including "[that] the Government [would] target the communications of non-U.S. persons with whom they communicate," that the Government would succeed in intercepting those communications, and that the plaintiffs would "be parties to the particular communications the Government intercepts." *Id.* at 1148–50. *Amnesty International* controls the disposition of this case, because Plaintiffs here have likewise made no well-pleaded, non-speculative allegations plausibly establishing that their online communications have been intercepted, copied

or reviewed for selectors at the alleged initial stages of Upstream collection, or that communications of theirs have been retained, read, and disseminated by the NSA.

Plaintiffs' allegation that their communications are intercepted, copied, and reviewed is predicated first on their conclusory assertion that the NSA intercepts, copies, and reviews for selectors "substantially all" international online communications carried in the U.S. But the Amended Complaint contains no factual enhancement to support this allegation, and under the plausibility standard of pleading announced in *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007), and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), it is not entitled to the assumption of truth.

Plaintiffs also allege that they "collectively" engage in more than a trillion online communications each year, and that their "sheer volume" and global distribution make it "virtually certain" that the NSA intercepts "at least one of the Plaintiffs' communications." But the Amended Complaint makes clear that the overwhelming number of these communications are communications involving Plaintiff Wikimedia Foundation ("Wikimedia") alone—the online transmissions of information that occur when individual Internet users visit Wikimedia websites. The other Plaintiffs cannot establish their standing based on an alleged certainty that Wikimedia's communications are intercepted and reviewed for selectors by the NSA.

Furthermore, Wikimedia's allegations regarding the volume and distribution of its websites' communications with Internet users fail to establish even its own standing. In an era when yearly Internet traffic is measured in tens, even hundreds of trillions of communications, Wikimedia's alleged "extraordinarily high volume of internet communications" is merely a drop in the torrent, and the claimed "99.9999999999%" certainty that the NSA intercepts its communications is statistically unsupported (indeed, contradicted) by Plaintiffs' own allegations. The related claim that the global distribution of Wikimedia's communications also makes interception by the NSA a virtual certainty, rests on erroneous assumptions about Internet

technology, as well as speculation about technical details of Upstream collection that remain classified, and that Plaintiffs could not attempt to confirm without implicating potential state secrets. *See Jewel v. NSA*, 2015 WL 545925 (N.D. Cal. Feb. 10, 2015). Moreover, Wikimedia identifies no privacy interest of its own in these communications; rather, it asserts that NSA surveillance invades the privacy of anonymous Internet users who view, download, or contribute information displayed on its public websites. Wikimedia lacks standing, however, to assert the legal rights and interests of these unidentified third parties.

Plaintiffs' further allegation, that it is "substantially likely" the NSA has also retained, read, and disseminated communications of theirs, likewise fails for two reasons. First, they have not plausibly alleged the interception of their communications to begin with. Second, claims that their communications are likely retained by the NSA because they communicate with probable targets of NSA surveillance echo the very factual claims that *Amnesty International* held were legally insufficient to establish Article III injury. In short, Plaintiffs' allegations rest on speculation concerning the focus and reach of Government intelligence-gathering programs, which *Amnesty International* teaches is insufficient to demonstrate standing.

For these reasons, discussed more fully below, Plaintiffs have not plausibly alleged facts establishing, with the genuine certainty required by *Amnesty International*, that they are suffering injury attributable to Upstream surveillance. Therefore they lack standing to contest the legality of this critical national-security program, and the Amended Complaint should be dismissed.

## BACKGROUND

### The Foreign Intelligence Surveillance Act

Congress enacted FISA in 1978 "to regulate the use of electronic surveillance within the United States for foreign intelligence purposes." S. Rep. No. 604, 95th Cong., 1st Sess., at 7 (1977). The statute was a response to revelations of unlawful Government surveillance directed

at specific U.S. citizens and political organizations. *Id*. at 7–8. FISA provides a check against such abuses by placing certain types of foreign-intelligence surveillance under FISC oversight.[1]

Before the Government may conduct "electronic surveillance," as defined in FISA, to obtain foreign-intelligence information, the statute generally requires the Government to obtain an order from a FISC judge. *See* 50 U.S.C. §§ 1803(a), 1804(a), 1805.[2] To obtain such an order, the Government must establish "probable cause to believe that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power," and that "each of the facilities or places at which the surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." *Id*. § 1805(a)(2).[3]

When Congress enacted FISA in 1978, it focused on the domestic collection of foreign-intelligence by limiting the definition of "electronic surveillance" regulated by FISA to the acquisition of communications to or from (or other information about) persons located *in the United States*. *Id.* § 1801(f). Congress intentionally excluded from FISA the vast majority of Government surveillance then conducted outside the U.S., even if it targeted U.S. persons abroad or incidentally acquired communications to or from U.S. persons or persons located in the U.S. *See* S. Rep. No. 701, 95th Cong., 2d Sess., at 7, 34–35, 71 (1978) (the Act "does not deal with

[1] The FISC is an Article III court comprised of 11 U.S. district judges, appointed by the Chief Justice of the United States, with authority to consider applications for and grant orders authorizing electronic surveillance and other forms of Government intelligence-gathering regulated by FISA. *See* 50 U.S.C. § 1803(a); *In re Motion for Release of Court Records*, 526 F. Supp. 2d 484, 486 (F.I.S.C. 2007).

[2] Generally speaking, "foreign intelligence information" as defined under FISA includes information relating to international terrorism and terrorist attacks, the international proliferation of weapons of mass destruction, and clandestine intelligence activities, conducted by foreign powers, as well as other information regarding foreign powers that relates to the national security or the foreign affairs of the United States. *Id.* § 1801(e).

[3] The statute defines "foreign power" and an "agent of a foreign power" to include non-U.S. persons and foreign entities "engaged in international terrorism or activities in preparation therefor," and those "engaged in the international proliferation of weapons of mass destruction." 50 U.S.C. § 1801(a)(4), (7); *id.* § 1801(b)(1)(C)–(E).

international signals intelligence activities" engaged in by the NSA or "electronic surveillance conducted" overseas); H.R. Rep. No. 1283(I), 95th Cong., 2d Sess., at 50–51 (1978).[4]

**The FISA Amendments Act of 2008**

In 2006, Congress began consideration of amendments to modernize FISA, because of changes in communications technology and the President's acknowledgment of the (now terminated) Terrorist Surveillance Program. S. Rep. No. 209, 110th Cong., 1st Sess., at 2–5 (2007); *see Amnesty Int'l*, 133 S. Ct. at 1143–44. As Congress concluded, FISA's definition of "electronic surveillance" was "tie[d] . . . to a snapshot of outdated technology." *Modernization of the FISA: Hearing before the S. Select Comm. on Intel*., 110th Cong., 1st Sess., at 19 (2007) ("FISA Modernization Hrg."). In 1978, Congress excluded international radio communications from FISA's definition of "electronic surveillance" to allow the Government to monitor international radio traffic outside FISA's confines, even when intercepted in the United States.[5] But whereas international communications were predominantly carried by radio or satellite when FISA was enacted, by the early 2000s they were predominantly carried by fiber-optic cables, and potentially qualified as wire communications subject to FISA when intercepted in the U.S. Thus, many international communications that generally would have fallen beyond FISA's ambit in 1978 were now potentially included, due merely to a change in technology. *Id.* at 18–19.

Further, with respect to wire or other non-radio communications, FISA's definition of electronic surveillance "place[d] a premium on the location of the collection": intercepts conducted inside the United States were covered, while those conducted outside the U.S.

[4] Electronic surveillance conducted by the Intelligence Community outside the United States is generally governed by Executive Order No. 12333, 46 Fed. Reg. 59941 (Dec. 4, 1981), reprinted as amended, 50 U.S.C. § 3001 note.

[5] *Compare* 50 U.S.C. § 1801(f)(2) (defining wire communication as "electronic surveillance" if, *inter alia*, one party is in the United States), *with id.* § 1801(f)(3) (defining radio communication as "electronic surveillance" only if all intended parties are in the United States).

generally were not. *Id.* at 19; 50 U.S.C. § 1801(f)(2). Technological advances had rendered this distinction outmoded too. "Legislators in 1978" had not predicted "an integrated global communications grid" on which a communication "can transit the world even if the two people communicating are only located a few miles apart." FISA Modernization Hrg. at 19. Due to these technological changes, the Government had to expend significant time and resources seeking FISC approval for surveillance that was originally intended to be outside FISA's scope, *id.* at 18, thus suffering delays that resulted in the loss of important foreign-intelligence information, *see* Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the FISA* ("PCLOB Report") (Exh. 1, hereto). The fix needed for this problem was a "technology-neutral" framework for surveillance of foreign targets, focused not on "how a communication travels or where it is intercepted," but instead on "who is the subject of the surveillance, which really is the critical issue for civil liberties purposes." FISA Modernization Hrg. at 46.

Congress ultimately addressed this problem through the FISA Amendments Act of 2008 ("FAA"), Pub. L. No. 110-261 (2008). The FAA added a new Title VII to FISA to establish procedures and requirements for the authorization of surveillance targeting persons located outside the United States. *See id.* § 101(a); 50 U.S.C. §§ 1881a-1881g. FISA section 702, 50 U.S.C. § 1881a, the provision implicated in this case, "supplements pre-existing FISA authority by creating a new framework under which the Government may seek the FISC's authorization of certain foreign intelligence surveillance targeting . . . non-U.S. persons located abroad," *Amnesty Int'l*, 133 S. Ct. at 1144, without regard to the location of the collection. 50 U.S.C. § 1881a(a), (b). Section 702 generally provides that upon the FISC's approval of a "certification" submitted by the Government, the Attorney General and the Director of National Intelligence may jointly authorize, for up to one year, the "targeting of [non-U.S.] persons

reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a), (b), (g). The statute expressly prohibits, however, the intentional targeting of any person known at the time of acquisition to be in the United States, or any U.S. person reasonably believed to be located outside the United States. *Id.* § 1881a(b). The acquisition must also be "conducted in a manner consistent with the [F]ourth [A]mendment." *Id.*

To meet the statutory requirements for FISC approval, the Government's certification must attest, *inter alia*, that a significant purpose of the acquisition is to obtain foreign-intelligence information either from or with the assistance of an electronic-communication-service provider. *Id.* § 1881a(g)(2)(A)(v), (vi). The Government must also certify that the acquisition will be conducted in accordance with targeting and minimization procedures meeting the statute's requirements. *Id.* § 1881a(d), (e), (g)(2)(B). Before approving a certification, the FISC must find that the Government's targeting procedures are reasonably designed (i) to ensure that acquisition is limited to targeting persons reasonably believed to be located outside the United States, and (ii) to prevent the intentional acquisition of wholly domestic communications. *See id.* § 1881a(d)(1), (i)(2)(B). The FISC must also find that the Government's minimization procedures are "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign-intelligence information." *Id.* § 1881a(i)(2)(C); *see also id.* §§ 1801(h), 1821(4). The FISC must also conclude that both the targeting and minimization procedures "are consistent with . . . the [F]ourth [A]mendment." *Id.* § 1881a(i)(3)(A). The Government's exercise of its authority under Section 702 and its compliance with statutory requirements are also subject to regular inter-agency reviews and assessments, and reporting to both the FISC and Congress. *Id.* § 1881a(l).

**Upstream Collection Under Section 702**

As the Plaintiffs observe, the collection of communications under Section 702 has been publicly described, in general terms, in a number of public Government reports and declassified FISC opinions. *See* First Amended Complaint for Declaratory and Injunctive Relief (ECF No. 70) (the "Amended Complaint," or "Am. Compl.") ¶ 37. Upon FISC approval of a certification under Section 702, NSA analysts identify non-U.S. persons located outside the United States who are reasonably believed to possess or receive, or are likely to communicate, foreign-intelligence information designated in the certification. Such a person might be an individual who belongs to a foreign terrorist organization or facilitates its activities. *See Liberty and Security in a Changing World*: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, at 136 (Dec. 12, 2013) ("PRG Report") (Exh. 2, hereto). Once the NSA has designated such a person as a target, it then attempts to identify a specific means by which the target communicates, such as an e-mail address or a telephone number, which is referred to as a "selector." Selectors may not be key words or the names of targeted individuals, but must be specific communications identifiers. *Id.*; PCLOB Report at 32–33, 36. To effect acquisition on appropriately identified selectors, the Government may issue a Section 702 "directive" to an electronic-communication-service provider in the United States requiring the provider to assist the Government in acquiring communications involving those selectors. 50 U.S.C. § 1881a(h); PCLOB Report at 32–33.

The NSA acquires communications associated with tasked selectors using two methods, known respectively as "Upstream" and "PRISM." *See* PCLOB Report at 33. Under PRISM collection, the Government notifies U.S.-based Internet service providers ("ISPs") of selectors identified for tasking, and the providers furnish the NSA with electronic communications to or from these selectors. *See id.* (Plaintiffs do not challenge PRISM collection in this case. *See*

Am. Compl. ¶ 40.) In contrast, Upstream involves the collection of communications as they transit the Internet "backbone" networks of U.S. telecommunications-service providers. *See* PCLOB Report at 35; PRG Report at 141 n.137. Tasked selectors are sent to providers operating these networks, whereupon they must assist the Government in acquiring communications to, from, or otherwise containing these selectors while they transit the "backbone." PCLOB Report at 36–37. Communications are filtered for the purpose of eliminating wholly domestic communications, and then scanned to capture communications containing tasked selectors. *Id*. at 37. Communications passing both these screens are ingested into NSA databases. *Id*. Further operational details regarding the mechanics of Upstream collection remain classified.

Upstream collection has been critical to Government efforts to combat international terrorism and other threats to the United States and its interests. Upstream is a "unique[ly] valu[able]" component of the Section 702 intelligence program, which "is critically important to maintaining our national security." PCLOB Report at 124; H.R. Rep. No. 645(II), 112th Cong., 2d Sess., at 3, 5 (2012); S. Rep. No. 174, 112th Cong., 2d Sess., at 2 (2012). The Section 702 program has "helped the United States learn more about the membership, leadership structure, priorities and plans of international terrorist organizations," "enabled the discovery of previously unknown terrorist operatives" and disruption "of previously unknown terrorist plots," and is also used to counter the proliferation of weapons of mass destruction. PCLOB Report at 107, 110.

**Plaintiffs' Allegations**

Plaintiffs are nine self-described "educational, legal, human rights, and media organizations" that allegedly "routinely engage in sensitive, confidential, and privileged internet communications with non-U.S. persons located abroad." Am. Compl. ¶¶ 2, 55, 78, 88, 93,102, 112-13, 130-31, 135-36, 140-41, 145-46, 150-51, 155-56, 160-61. Plaintiffs allege that they "collectively" engage in "more than a trillion" such communications "over the [I]nternet each

year," with individuals "in virtually every country on [E]arth," *id.* ¶¶ 2, 58, 60, 88. Plaintiffs maintain that "[t]he ability to exchange information in confidence, free from warrantless government monitoring, is essential to [their] work," and that Upstream collection "violates [their] privacy and undermines their ability to carry out activities crucial to their missions." *Id.* ¶¶ 2, 70, 76, 89, 108-10, 118, 129, 134, 139, 144, 149, 154, 159, 164. Plaintiffs sue on behalf of themselves and, purportedly, their staffs. *Id.* ¶¶ 6–14. Plaintiff National Association of Criminal Defense Lawyers ("NACDL") also purports to sue on behalf of its members. *Id.* ¶ 7.[6]

According to Plaintiffs, the NSA conducts Upstream surveillance "by connecting surveillance devices to multiple major [I]nternet cables, switches, and routers on the [I]nternet backbone," the international submarine and high-capacity terrestrial cables "that carry [I]nternet communications into and out of the United States," *id.* ¶¶ 46, 47, 60. Plaintiffs allege that Upstream "is intended to enable the comprehensive monitoring of international [I]nternet traffic," allowing the NSA to "cop[y] and review[ ] all international e-mails and other 'text-based' communications." *Id.* ¶ 48. Plaintiffs describe Upstream as encompassing four processes: (1) copying, during which "the NSA makes a copy of substantially all international text-based communications"; (2) filtering, during which "[t]he NSA attempts to filter out and discard some wholly domestic communications from the stream of internet data"; (3) content review of the copied communications—"including their full content—for instances of [the NSA's] search terms [selectors]"; and (4) retention by the NSA of "all communications that contain selectors associated with its targets, as well as those that happened to be bundled with them in transit," for further review and analysis and dissemination of the results. *Id.* ¶ 49.

[6] Six of the Plaintiffs, Human Rights Watch, Amnesty International USA, the PEN American Center, the Global Fund for Women, the Nation Magazine, and the Washington Office on Latin America, were also plaintiffs in *Amnesty International*. *See* Compl. ¶¶ 8–12, 14; *Amnesty Int'l USA v. Clapper*, 638 F.3d 118 (2d Cir. 2011), *rev'd*, 133 S. Ct. 1138 (2013).

Based on the allegation that Upstream surveillance involves "intercepting, copying, and reviewing substantially all international text-based communications . . . as they transit telecommunications networks inside the United States," Plaintiffs assert that the NSA intercepts, copies, and reviews for selectors the international online communications in which their staffs (or, in NACDL's case, its members) engage in furtherance of their organizational (or professional) missions. Am. Compl. ¶¶ 56, 103, 113-14, 131-32, 136-37, 141-42, 146-47, 151-52, 156-57, 161-62; *see also id.* ¶¶ 1, 38, 40, 48, 49, 50. Wikimedia also alleges that the NSA intercepts, copies, and reviews two other categories of "Wikimedia['s] communications," specifically: (1) the allegedly more than one trillion annual "communications" that occur when individuals, "located in virtually every country on [E]arth," view Wikimedia websites to "read and contribute to [them] and [to] use [them] to interact with each other"; and (2) Wikimedia's "logs" of online requests by such users to view its webpages. *Id.* ¶¶ 81, 86, 88, 93.

According to Plaintiffs, their claim that the NSA intercepts, copies, and reviews their communications is also "well-founded," Am. Compl. ¶ 57, because of (1) the "sheer volume" of their international online communications, *id.* ¶ 58; (2) the "geographic distribution" of their communications "across the globe," *id.* ¶¶ 60-61; (3) the manner in which the NSA "must be" conducting Upstream surveillance to "reliably obtain" all communications to, from, or about its targets, *id.* ¶¶ 62-64; and (4) the Government's alleged "strong incentive" to intercept communications at as many Internet backbone "chokepoints" as possible, *id.* ¶ 65.

Plaintiffs maintain that the alleged interception, copying and selector review of their communications invades their privacy and the privacy of their staffs, Wikimedia's users, and NACDL's members, and infringes on "their right to control [their] communications and the information they contain." Am. Compl. ¶¶ 103, 114, 132, 137, 142, 147, 152, 157, 162.

In addition to the claimed interception, copying, and selector review of their communications, Plaintiffs also allege that there is a "substantial likelihood" that their intercepted communications (in the case of NACDL, its members' communications) are "retained, read, and disseminated" by the NSA. *Id.* ¶ 71. The retention, analysis, and dissemination of their communications is likely, Plaintiffs maintain, because they allegedly communicate online with people "whom the [G]overnment is likely to target when conducting Upstream surveillance," and a "significant amount of the information" they exchange with those persons constitutes "foreign intelligence information" within the meaning of FISA. *Id.* ¶¶ 73–74; *see also id.* ¶¶ 104-07, 115, 124-27, 133, 138, 143, 148, 153, 158, 163. Plaintiffs contend the alleged "retention, reading, and dissemination of Plaintiffs' communications is a further, discrete violation of [their] reasonable expectation of privacy in those communications," and of their "right to control those communications and the information they reveal and contain." *Id.* ¶ 72.

Plaintiffs further allege that Upstream surveillance "undermines their ability to carry out activities crucial to their missions," first by forcing them "to take burdensome and sometimes costly measures to minimize the chance that the confidentiality of their sensitive information will be compromised," and second by "reduc[ing] the likelihood that . . . individuals will share sensitive information with [them]." Am. Compl. ¶¶ 2, 75, 76; *see also id.* ¶¶ 108, 109, 118, 128, 129, 134, 139, 144, 149, 154, 159, 164. Plaintiffs contend that Upstream surveillance exceeds the Government's authority under Section 702 and violates the First and Fourth Amendments and Article III of the Constitution. *Id.* ¶¶ 165–168. By way of relief, Plaintiffs seek a declaration that Upstream surveillance is unlawful, an injunction prohibiting Upstream surveillance of their communications, and a purge from Government databases of any of their communications acquired through Upstream surveillance. *Id.* ¶ 3; *id.* at 55-56 (prayer for relief).

## ARGUMENT

## I. LEGAL STANDARDS

### A. Pleading Standards Under *Twombly* and *Iqbal*

The Amended Complaint must be dismissed for lack of subject-matter jurisdiction, because it contains no well-pleaded allegations that plausibly establish Plaintiffs' standing. To withstand a motion to dismiss, a complaint must contain "sufficient factual matter, accepted as true, to 'state a claim that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)); *Vitol, S.A. v. Primerose Shipping Co.*, 708 F.3d 527, 543 (4th Cir. 2013). Mere "labels and conclusions" and "naked assertion[s] devoid of further factual enhancement" are not sufficient. *Iqbal*, 556 U.S. at 678. Rather, a court must disregard "pleadings that, because they are no more than conclusions, are not entitled to the assumption of truth," and determine whether the remaining "well-pleaded factual allegations . . . plausibly give rise to an entitlement to relief." *Id.* at 679; *see id.* at 680–81; *Vitol*, 708 F.3d at 543. The plausibility standard of pleading applies to both the elements of a claim and the plaintiff's allegations of standing. *See David v. Alphin*, 704 F.3d 327, 333 (4th Cir. 2013). A court will find that a complaint plausibly alleges standing only if the "well-pleaded allegations" allow it to "draw the reasonable inference"—and do not merely give rise to a "sheer possibility," *Iqbal*, 556 U.S. at 678–79—that the plaintiff has standing. *David*, 704 F.3d at 333; *Zander v. United States*, 786 F. Supp. 2d 880, 883 (D. Md. 2011).

### B. The Requirements of Standing

"The judicial power of the United States . . . is not an unconditioned authority to determine the [validity] of legislative or executive acts," but is limited by Article III of the Constitution "to the resolution of 'cases' and 'controversies.'" *Valley Forge Christian Coll. v. Americans United for Separation of Church & State, Inc.*, 454 U.S. 464, 471 (1982); *Burke v.*

*City of Charleston*, 139 F.3d 401, 404 (4th Cir. 1998). A demonstration by plaintiffs of their standing to sue "is an essential and unchanging part of the case-or-controversy requirement," *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992), and as such is a threshold jurisdictional requirement, "determining the power of the court to entertain the suit." *Warth v. Seldin*, 422 U.S. 490, 498–99 (1975). The Supreme Court emphasized in *Amnesty International* that the standing inquiry must be "especially rigorous when reaching the merits of the dispute would force [a court] to decide whether an action taken by one of the other two branches of the Federal Government," particularly "in the fields of intelligence gathering and foreign affairs," "was unconstitutional." 133 S. Ct. at 1147 (citations omitted).

To establish Article III standing, Plaintiffs must seek relief from an injury that is "'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'" *Id.* As "[t]he part[ies] invoking federal court jurisdiction," Plaintiffs "bear[ ] the burden of establishing these elements." *Doe v. Va. Dep't of State Police*, 713 F.3d 745, 753 (4th Cir. 2013). The alleged injury must be "real and immediate," not "conjectural or hypothetical," *Shenandoah Valley Network v. Capka*, 669 F.3d 194, 202 (4th Cir. 2012) (citations omitted). Speculative claims of injury will not support Article III standing. *Amnesty Int'l*, 133 S. Ct. at 1150; *see Stephens v. Cnty. of Albermarle, Va.*, 524 F.3d 485, 492–93 (4th Cir. 2008).

In addition to "'constitutional limitations on federal-court jurisdiction,'" the standing inquiry "involves . . . 'prudential limitations on its exercise.'" *Kowalski v. Tesmer*, 543 U.S. 125, 128–29 (2004) (quoting *Warth*, 422 U.S. at 498); *Freilich v. Upper Chesapeake Health, Inc.*, 313 F.3d 205, 214–15 (4th Cir. 2002). Among these prudential limitations is "the rule that a party 'generally must assert [its] own legal rights and interests, and cannot rest [its] claim to relief on the legal rights or interests of third parties.'" *Tesmer*, 543 U.S. at 129 (quoting *Warth*,

422 U.S. at 499); *Valley Forge*, 454 U.S. at 474 (same); *Doe*, 713 F.3d at 753 ("[T]he Supreme Court has explained that prudential standing encompasses the general prohibition on a litigant's raising another person's legal rights.") (citation omitted).

Plaintiffs' assertions of injury are essentially two-fold. They first claim injury based on the alleged "interception, copying, and review" of their communications during the Upstream process, and second claim an additional discrete injury based on the alleged "substantial likelihood" that communications of theirs are "retained, read, and disseminated" by the NSA. Am. Compl. ¶¶ 70–71. The first of these claims of injury rests on the wholly conclusory assertion that the NSA intercepts substantially all international online communications transiting the United States, alleged statistical "certainties" based on hypothetical premises, and other stated and unstated assumptions about the manner in which the NSA "must be" conducting Upstream surveillance, for which the Amended Complaint offers no supporting factual allegations. It amounts therefore, to nothing more than a speculative claim of injury that *Amnesty International* teaches will not support Article III standing. Plaintiffs' second claim of injury simply repeats the very allegations that the Supreme Court held were legally insufficient in *Amnesty International*. For these and the further reasons discussed below, Plaintiffs have not plausibly alleged injuries to their own legal rights that are fairly traceable to Upstream surveillance. Their claims challenging Upstream surveillance must therefore be dismissed.

## II. PLAINTIFFS HAVE NOT PLAUSIBLY ALLEGED THAT THEY HAVE BEEN INJURED BY THE INTERCEPTION, COPYING, AND REVIEW OF THEIR ONLINE COMMUNICATIONS IN THE UPSTREAM COLLECTION PROCESS.

### A. Plaintiffs Have Not Plausibly Alleged That Upstream Collection Involves the Interception, Copying, and Selector Review of Substantially All International Online Communications Transiting the United States.

Plaintiffs' claims that they are injured through alleged NSA interception, copying, and selector review of online communications are insufficient to establish the requisite Article III

injury, because they have not plausibly alleged that any of *their* online communications are intercepted, copied, or reviewed during the Upstream process. As discussed *supra*, at 11, Plaintiffs allege that Upstream collection involves initial interception and copying of online communications to review them for selectors (such as e-mail addresses) associated with targets of NSA surveillance; communications found to contain such selectors are thereafter retained in NSA databases for further analysis. Am. Compl. ¶¶ 42–43. The assertion that *their* communications are intercepted, copied and reviewed is first predicated on the "bald allegation[ ]," *Iqbal*, 556 U.S. at 681, that the NSA intercepts, copies, and reviews "substantially all international [online] communications . . . as they transit telecommunications networks inside the United States." *Id.* ¶¶ 1, 38, 48-50, 56, 103, 114, 132, 137, 142, 147, 152, 157, 162.

But this "bare assertion[ ]" is unaccompanied by "factual matter" that raises it "above the speculative level," and as such it is neither entitled to the presumption of truth nor sufficient, therefore, to state a plausible claim of standing. *Iqbal*, 556 U.S. at 681; *Twombly*, 550 U.S. at 555. Plaintiffs, for example, cite no statements by Government officials acknowledging that Upstream involves the collection of all (or substantially all) international online communications transiting the United States. To the contrary, Upstream's scope and the scale on which it operates remain classified. Thus, Plaintiffs can only speculate whether the NSA has ever intercepted, collected, or reviewed their communications for selectors in conducting Upstream surveillance. *Amnesty International* makes clear that injury so speculative and conjectural is insufficient to establish Article III standing, especially the standing of litigants who ask the courts to determine the constitutionality of the Government's actions in the field of foreign intelligence. *Amnesty Int'l*, 133 S. Ct. at 1147–50; *see also Stephens*, 524 F.3d at 493.

The Amended Complaint refers to a number of public Government reports and recently declassified FISC opinions which, according to Plaintiffs, "indicate that FAA surveillance results

in the wide-ranging and persistent interception of U.S. persons' communications." Am. Compl. ¶ 37. But a nebulous allegation that "FAA surveillance" is "wide-ranging" stops far short of plausibly establishing that Upstream surveillance involves the interception, copying, and review for selectors of all or even "substantially all," *id.* ¶¶ 1, 48, international online communication carried on U.S. networks. *Twombly*, 550 U.S. at 556–57. This is especially so considering that Upstream, the only surveillance program challenged by Plaintiffs, is just one of the programs conducted under authority of the FAA. *See supra*, at 10; Am. Compl. ¶¶ 39–40.

The public documents alluded to by Plaintiffs fall short in the same ways. Plaintiffs refer to a report by the Office of the Director of National Intelligence ("ODNI"), which estimates that in 2014 the Intelligence Community relied on Section 702 to conduct surveillance of 92,707 persons, groups, or organizations. Am. Compl. ¶ 37; *see* ODNI, Statistical Transparency Report Regarding Use of National Security Authorities (April 22, 2015) ("ODNI Transparency Report") (Exh. 3, hereto) at 1, 2.[7] This figure lends no support to the allegation that Upstream collection involves the interception of all international online communications traversing U.S. providers' networks. First, the report does not reveal how many of these 92,707 persons, groups, and organizations were targets of Upstream as opposed to PRISM surveillance. ODNI Transparency Report at 1. But even if all 92,707 were targets of Upstream collection (out of roughly three billion Internet users worldwide, *see* Declaration of Robert T. Lee[8] (attached hereto) ("Lee

[7] In ruling on a motion to dismiss, a court may "consider documents incorporated into the complaint by reference." *United States ex rel. Oberg v. Pa. Higher Educ. Assistance Agency*, 745 F.3d 131, 136 (4th Cir. 2014) (citation omitted).

[8] Mr. Lee is a consultant "specializing in information security, incident response, and digital forensics." Lee Decl. ¶ 1. With more than 15 years of experience in, *inter alia*, computer forensics, vulnerability, and intrusion detection/prevention," Mr. Lee is currently the curriculum lead for digital forensic and incident response training at the SANS Institute. *Id.* Previously, he served in the U.S. Air Force in a unit focused on information warfare, and "led a team conducting computer crime investigations, incident response, and computer forensics." *Id.* He

Decl.") ¶ 25)[9] that says nothing about the scale on which Upstream collection is conducted to maintain surveillance on those targets. Thus it fails to raise the claim that the NSA intercepts, copies, and reviews for selectors all international online communications sent or received in the U.S. "above the speculative level." *Twombly*, 550 U.S. at 555.

Plaintiffs also point to a now declassified opinion in which the FISC, conducting review of the NSA's targeting and minimization procedures for Upstream collection, observed that the NSA annually collected more than 250 million online communications pursuant to Section 702. Am. Compl. ¶ 37; [*Caption Redacted*], 2011 WL 10945618, at *9 (F.I.S.C. Oct. 3, 2011) ("Oct. 3, 2011 FISC Op.").[10] The FISC also found, however, "[that] the vast majority of these communications [were] obtained from Internet service providers" via PRISM collection, not Upstream. *Id.* at *9 & n.24. "Indeed, NSA's [U]pstream collection constitute[d] only approximately 9% of the total Internet communications [then] acquired by [the] NSA under Section 702," *id.* at *9; *see also id.* at *7 n.21, *26, or roughly 25 million communications out of the many trillions that traverse the Internet each year. *See* Lee Decl. ¶¶ 27-3213–19. Nothing in the FISC's October 3, 2011 opinion suggests that the NSA, in order to collect this tiny

---

has worked with law enforcement and the intelligence community "as a technical lead" on projects including "computer forensic and security software development" and "cyber-forensics." *Id.* Mr. Lee has also co-authored a book in this field, *Know Your Enemy* (2d ed.).

[9] When subject matter jurisdiction is challenged via a Rule 12(b)(1) motion to dismiss, "the district court . . . may consider evidence outside the pleadings without converting the proceeding to one for summary judgment." *Velasco v. Gov't of Indonesia*, 370 F.3d 392, 398 (4th Cir. 2004); *Murphy-Taylor v. Hofmann*, 968 F. Supp. 2d 693, 712 (D. Md. 2013).

[10] In that decision the FISC largely approved the NSA's targeting and minimization procedures as consistent with statutory and constitutional requirements, but concluded that they fell short so far as "multi-communication transactions" were concerned. Oct. 3, 2011 FISC Op., 2011 WL at 10945618, at *5–6. Thereafter the NSA amended its procedures, and the FISC concluded the amendments "[had] adequately corrected the deficiencies identified" in its October 3, 2011 opinion. [*Caption Redacted*], 2011 WL 10947772, at *8 (F.I.S.C. Nov. 30, 2011).

percentage of online communications, first intercepts, copies, and reviews for selectors almost every international communication carried on U.S. telecommunications networks.

Lastly, Plaintiffs rely on the PCLOB and PRG Reports, Am. Compl. ¶ 37, but these reports simply repeat the figures in the ODNI Transparency Report and the FISC's October 3, 2011 opinion. *See* PCLOB Report at 33 & n.116, 37 & n.134, 113, 116 n.487; PRG Report at 142. They add nothing regarding the scope or scale on which Upstream collection operates.

In short, Plaintiffs' "naked assertions" are unsupported by any well-pleaded, non-conclusory allegations from which it could plausibly be concluded that the NSA, when conducting Upstream surveillance, intercepts, copies, and reviews for selectors "substantially all" international online communications that traverse the United States. Consequently, they have failed to plausibly allege interception, copying, or review of their communications so as to support their Article III standing. *Iqbal*, 556 U.S. at 678; *Southern Walk at Broadlands Homeowner's Ass'n, Inc. v. Open Band at Broadlands, LLC*, 713 F.3d 175, 182 (4th Cir. 2013).

**B. Neither the Alleged "Extraordinarily High Volume" and Global Distribution of Wikimedia's Communications, Nor Plaintiffs' Unilateral Assumptions About How Upstream Surveillance "Must Be" Conducted To Achieve Its Objectives, Establishes That Any of the Plaintiffs' Communications (Including Wikimedia's) Are Intercepted, Copied, or Reviewed for Selectors in the Upstream Collection Process.**

Plaintiffs next allege that the "sheer volume" and "geographic distribution" of their online communications also make it "virtually certain" that the NSA intercepts, copies and reviews for selectors "at least some of their communications." Am. Compl. ¶¶ 58-67. First, they assert that because Plaintiffs "collectively engage" in more than a trillion international online communications each year, "the odds of the [NSA] copying and reviewing at least one of the Plaintiffs' communications in a one-year period [is] greater than 99.9999999999 %." *Id.* ¶ 58. And because Plaintiffs allegedly communicate "with individuals in virtually every country on [E]arth," they assert that "[their] communications almost certainly traverse every international

backbone link connecting the United States with the rest of the world," at least some of which, they maintain, are "monitor[ed]" by the NSA. *Id.* ¶¶ 61, 63.

As explained below, these allegations are also insufficient to establish that any of the Plaintiffs' communications are intercepted, copied and reviewed by the NSA. The Amended Complaint makes plain that when Plaintiffs speak of the alleged volume and global distribution of their "collective[ ]" communications they effectively mean the data transmissions that occur when anonymous Internet users from around the world view and download pages on Wikimedia websites. *See id.* ¶ 88. The eight other Plaintiffs cannot base their standing, however, on the alleged interception, copying, and review of Wikimedia's communications. *See* § II.B.1, *infra.*

Moreover, Plaintiffs' allegations fail even to establish Wikimedia's standing. The alleged number of page views on Wikimedia's websites represents a relatively small portion of total Internet traffic, and the claim that the volume of these page views makes it over 99% certain that the NSA is intercepting, copying, and reviewing even Wikimedia's communications is statistically unsupported—indeed, contradicted—by the Amended Complaint's allegations. *See* §§ II.B.2, B.3, *infra.* Likewise, the proposition that the alleged worldwide distribution of requests to view Wikimedia webpages also makes it virtually certain that Wikimedia's "communications" are intercepted, copied and reviewed for selectors, Am. Compl. ¶¶ 62-65, rests on unsupported speculation about how the NSA "must be" conducting Upstream surveillance to achieve its supposed objectives. *See* § II.B.4, *infra*. Under *Amnesty International*, the statistical assumptions and speculation on which Plaintiffs rely are insufficient, as a matter of law, to establish the injury required for purposes of Article III. *See* § II.B.5, *infra.*

#### 1. Wikimedia's Co-Plaintiffs Cannot Base Their Standing on the Alleged Number and Distribution of Visits to Wikimedia Websites.

The Amended Complaint alleges that "[i]n the course of a year, Plaintiffs"—nine entities in all—"collectively engage in more than one trillion international [I]nternet communications,"

and that they "communicate with individuals in virtually every country on [E]arth." Am. Compl. ¶¶ 58, 61. In Plaintiffs' view, the "sheer volume" and "geographic distribution" of the communications in which they "collectively" engage make it "virtually certain that the NSA has intercepted, copied, and reviewed Plaintiffs' communications." *Id.* ¶¶ 58, 60.

The Amended Complaint makes it clear, however, that the vast majority of the online communications in which Plaintiffs say they "collectively" engage are communications in which Wikimedia alone claims to engage, the data transmissions that occur when Internet users view or download information appearing on Wikimedia's public websites. Plaintiffs allege that Wikimedia alone "engages in more than one trillion international communications each year, with individuals who are located in virtually every country on [E]arth," based on the alleged 88 billion monthly requests it receives from Internet users outside the United States to view, download, or edit the content on Wikimedia websites. *Id.* ¶ 88; *see also id.* ¶ 87 ("As the operator of one of the most-visited websites in the world [Wikipedia], Wikimedia engages in an extraordinarily high volume of [I]nternet communications.").

Thus, the face of the Amended Complaint itself makes clear that when Plaintiffs speak of the "more than one trillion international [I]nternet communications" in which they "collectively engage," *id.* ¶ 58, they mean the more than one trillion so-called communications in which Wikimedia alone engages, plus the relatively inconsequential numbers of each of the other Plaintiffs' online communications, which the Amended Complaint does not even bother to quantify. But even if the "sheer volume" and distribution of Wikimedia's communications were sufficient to establish Wikimedia's standing—which, as discussed in §§ II.B.2, B.3, *infra*, it is not—it proves nothing about the likelihood of intercepting the communications of the other eight Plaintiffs. *See Valley Forge*, 454 U.S. at 472 ("Art[icle] III requires [a] party who invokes the court's authority to show that [it] personally has suffered some actual or threatened injury . . . .")

(citation omitted); *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 39 (1976) (a party seeking judicial review "must [it]self have suffered an injury").

Plaintiffs maintain that because of the "collective[]" volume of their communications, the odds are at least "99.9999999999%" that the NSA intercepts, copies, and reviews "*at least one of the Plaintiffs'* communications in a one-year period." Am. Compl. ¶ 58 (emphasis added). But even if that claim were statistically supported by Plaintiffs' allegations—which it is not, *see* § II.B.2, *infra*—the chances that the NSA intercepts, copies, and reviews "at least one communication for a particular Plaintiff" other than Wikimedia are "likely much lower." Declaration of Dr. Alan Salzberg (attached hereto) ("Salzberg Decl.") ¶ 12.[11] For example, even accepting Plaintiffs' assumptions, *see* Am. Compl. ¶ 58, if another of the Plaintiff organizations conducted as many as one million online communications each year, "the chances that at least one of that Plaintiff's communications (as opposed to Plaintiff Wikimedia's communications) would be [intercepted,] copied, and reviewed would be [just] 1 in 10,000." Salzberg Decl. ¶ 13.

Moreover, Plaintiffs' communal theory of injury, that all of them have standing because "at least one of [their] communications" statistically must have been intercepted, is foreign to the principles of standing. "Standing is not dispensed in gross." *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs.*, 528 U.S. 167, 185 (2000) (quoting *Lewis v. Casey*, 518 U.S. 343, 358 n.6 (1996)). "It is not enough [to show] that the conduct of which [a] plaintiff complains will injure someone," *Blum v. Yaretsky*, 457 U.S. 991, 999 (1982); rather, "[a] party seeking review [must] be [it]self among the injured." *Defenders of Wildlife*, 504 U.S. at 563. It does not meet any of

[11] Dr. Salzberg is the Principal (and owner) of Salt Hill Statistical Consulting. He received a Ph.D. in Statistics from the University of Pennsylvania, has taught courses in statistics and quantitative methods at the University of Pennsylvania and American University, has published several statistics papers in peer-reviewed journals, and is the co-inventor of a patented statistical process designed to test the systems of telecommunications companies. Dr. Salzberg's work involves statistical sampling, analysis, and review conducted in a wide variety of matters for government and industry. Salzberg Decl. ¶¶ 1-3.

the Plaintiffs' burden under Article III to allege that "at least one" of them has been injured without specifying which one (or more) of them, if any, has (or have) actually suffered concrete harm because of the Government's alleged conduct. *Cf. Summers v. Earth Island Inst.*, 555 U.S. 488, 497-99 (2009) (even a "statistical probability that some of [an organization's] members are threatened with concrete injury" could not establish the organization's standing absent "specific allegations establishing that at least one identified member had suffered or would suffer harm").

**2. Wikimedia's Alleged International Online Communications Represent Only a Small Proportion of the Total Volume of Communications Carried on the Internet.**

The "sheer volume" of Wikimedia's international online communications, allegedly "more than one trillion . . . each year," Am. Compl. ¶ 88, also fails to support an inference, much less establish a certainty, that the NSA intercepts, copies, and reviews any of Wikimedia's communications. *Id.* ¶ 58. Traffic on the Internet includes numerous forms of communications, including "e-mail, web browsing, social media, audio and video streaming, Voice Over Internet Protocol (Internet telephony), video conferencing, and peer to peer sharing." Lee Decl. ¶ 26. This traffic totals about 2.4 billion gigabytes of data traversing the Internet per day, about 875 billion gigabytes per year. *Id.* Wikimedia does not plead what portion of these communications, even the text-based communications, *see id.* ¶¶ 26-34, may be attributed to its communications. In other words, Wikimedia provides no context with which to evaluate whether a trillion Internet "communications" constitutes a comparatively large or comparatively small share of the total.[12]

Wikimedia appears to calculate its alleged one trillion international online "communications" by totaling the number of HTTP (or HTTPS) (hereinafter HTTP/S)[13]

[12] Put simply, Wikimedia has told the Court how many drops of water it has in the bucket, without telling the Court how much water is in the bucket.

[13] An HTTP request is a means of asking for data transfer on the Internet; if the communication stream is encrypted, the request is an HTTPS request. Lee Decl. ¶ 18 & nn.7-8.

"requests" that Wikimedia websites receive when users "view, search, log in [to], edit, or contribute to a Wikimedia Project webpage," Am. Compl. ¶ 88, the sites' responses thereto, and the number of "corresponding log entr[ies]" that the sites create to track each of those requests. *Id.* ¶ 93.[14] Wikimedia alleges that its U.S.-based servers received more than 88 billion HTTP/S requests in May 2015, equating to more than one trillion a year, *see id*. ¶ 88.

The number of HTTP/S requests, however, is not a reliable measure of the relative volume of a website's traffic. Webpages may consist of many, even hundreds, of files depending on their complexity and graphic content. When a user sends a request to view a webpage, the website's host computers send each of the files comprising that webpage in a separate HTTP/S transmission. Lee Decl. ¶ 18. Thus, for example, to permit a user "to view a webpage containing fifteen graphics, the webpage's host computer (or computers) would send sixteen files to the user's computer—one file to convey the text, and fifteen files to convey each of the images appearing on that page." *Id.* Because the number of HTTP/S requests a page view will generate depends on such factors as the number of graphics and advertisements on a webpage, *see id.* ¶ 32 n.34, they are "not a reliable metric for determining the comparative popularity and usage of websites," *id.* ¶ 18 n.8, and thus not a reliable baseline for comparing the volume of Wikimedia's "communications" (as Plaintiffs define that term) to that of other websites.

A more reliable metric, and one relied on by private industry to track website usage, is webpage views. Lee Decl. ¶¶ 24, 30. Wikimedia alleges that from "April 1, 2014 to March 31,

[14] Wikimedia also alleges that it "engages in communications that permit its users to interact with one another more directly" such as by "send[ing] an e-mail via Wikimedia to another registered user." Am. Compl. ¶ 92. Similarly, Wikimedia alleges that it "allows users to interact in small or limited groups" and "[s]ome of these communications are transmitted by HTTP or HTTPS." *Id.* Wikimedia also alleges that its "staff" also engages in online communications. *Id.* ¶ 86. Since the Amended Complaint does not purport to quantify these communications separate and apart from the alleged total of one trillion, presumably their number is minuscule in comparison to the volume of Wikimedia's Internet traffic.

2015, [its] websites received over 255 billion page views," Am. Compl. ¶ 87, that is, approximately 21.25 billion per month. These numbers, while apparently large, pale in comparison to the number of page views for other websites. Similar Web, one of a number of commercial organizations that track website usage, ranks Wikipedia (Wikimedia's most popular site) as number eight worldwide, *id.* ¶¶ 30-31, behind such Internet giants as Facebook.com and Google.com. *Id.* According to Similar Web, Facebook.com had an estimated 354 billion web page views per month in June 2015, or about 4.2 trillion each year; and Google.com had about 207 billion web page views per month, or about 2.5 trillion per year. *See id.* ¶ 31.[15]

Similar Web also publishes monthly page view data for the top 50 websites; in June 2015, the monthly total for the top 50 sites was 1.167 trillion, or 14 trillion per year, *see* Lee Decl. ¶ 32 & Exh. T, compared to Wikimedia's alleged monthly total of 21.25 billion, or 255 billion per year. Am. Compl. ¶ 87.[16] Thus, Wikimedia's "extraordinarily large" number of page views equals less than two percent (1.82%) of the views on the top 50 websites alone. That proportion "would fall much further if the total monthly page views of the approximately 244 million currently active websites" were known and used to calculate Wikimedia's share instead. Lee Decl. ¶ 32.

Wikimedia's 21.25 billion page views per month also pale in comparison to the total number of other text-based communications on the Internet, principally e-mail. Recent data

[15] If HTTP/S requests were used as the basis for comparison instead of page views, the volume of Wikimedia's communications would appear even smaller in relation to sites such as Facebook. This is so because "[t]ypically . . . a single page view on a site like Facebook.com, which contains many graphics and advertisements, will require many more HTTP requests than a page view on a text-heavy site, like Wikipedia, with few graphics and no ads." Lee Decl. ¶ 32 n.34; *see also id.* ¶ 18.

[16] Accepting Wikimedia's alleged 21.25 billion page views per month as a basis for comparison is likely generous to Wikimedia. Similar Web estimates that Wikipedia, by far the most popular of the Wiki projects, received only 7.92 billion page views in June 2015. Lee Decl. ¶ 31. None of Wikimedia's other websites ranks among the top 50 sites, *see id.*, Exh. T. It is unlikely they collectively receive nearly 14 billion page views per month.

indicate that approximately 207 billion e-mails are sent *every day*, *see* Lee Decl. ¶ 27, that is, about 6.21 trillion per month, or 75.6 trillion per year. Thus, Wikimedia's alleged volume of page views corresponds to approximately three-tenths of one percent (0.34%) of just the e-mail traffic carried on the Internet. *See id.* ¶ 28. Wikimedia's page views amount to less than three-tenths of a percent (0.29%) of the combined traffic attributable to e-mail (75 trillion) and the top 50 websites (14 trillion). *Id.* ¶ 33.

In short, Wikimedia's "extraordinarily high volume of internet communications" is minuscule when compared to the total volume of Internet traffic. Regardless of its "sheer volume," Wikimedia's "comparatively small" share of Internet traffic, Lee Decl. ¶ 34, does not itself plausibly establish a "virtual[ ] certain[ty]" that Wikimedia's communications are intercepted, copied, and reviewed during the Upstream process.

**3. Wikimedia's Allegation That the Volume of its Communications Makes Interception of at Least Some of Those Communications a Virtual Certainty is Statistically Unsupported.**

Notwithstanding its diminutive share of total Internet traffic, Wikimedia alleges that the "odds of the [NSA] copying and reviewing at least one of [its] communications in a one-year period would be greater than 99.9999999999%." Am. Compl. ¶ 58. While this figure gives the appearance of near statistical certainty, it rests on explicit and implicit assumptions which, if incorrect, would invalidate Plaintiffs' calculation, *see* Salzberg Decl. ¶¶ 4-6, yet for which the Amended Complaint gives no factual support. Critical assumptions underlying the calculation are in fact contradicted by Plaintiffs' allegations, such that the chances of copying and reviewing one of Wikimedia's communications "could be far less than 100%." *See id.* ¶¶ 11, 18—20.

Plaintiffs' calculation depends on two implied yet "sweeping" assumptions that lack "statistical foundation" in the Amended Complaint. *Id.* ¶¶ 5, 14, 15, 16. These two assumptions are of "'independence'" and "identical distribut[ion]," meaning that "the chances of copying and

reviewing" communications "are the same for all communications and that the chances of any one [communication] being copied and reviewed does not vary based on whether any other [communication] is copied and reviewed." *Id.* ¶ 14.[17] In practice, this two-fold assumption would mean that "communications from anywhere in the world all have equal chances of being copied and reviewed," whether a communication originates in Iran or Ireland. *Id.* Similarly, it means that a communication from someone's computer in Iran has no greater or lesser chance of being copied and reviewed than a communication "one second later" by someone using the same computer in Iran. *See id.* For Plaintiffs' calculation to be accurate, Upstream surveillance, in practice, would have to conform to this "studiously random statistical model." *Id.* ¶ 18.

But that is not how Plaintiffs have alleged that Upstream collection operates. *See id.* ¶¶ 14, 18, 19. In fact, Plaintiffs' "statistical assumptions . . . are inconsistent with how they say [the] . . . process works." *Id.* ¶ 18. Plaintiffs maintain that Upstream involves the installation of surveillance devices "at key access points" so that copying occurs at "*certain* high-capacity cables, switches, and routers." Am. Compl. ¶ 49 (emphasis added). "Any [resulting] clustering of the copying and reviewing of communications, whether by country or some other criteria, would mean [1] that some groups [of communications] would have different chances of being copied than some other groups and [2] that the fact that a particular communication in one group is reviewed or copied means [that] other communications in that group are more likely to be copied." Salzberg Decl. ¶ 15. In this way, "even a very large operation of copying and reviewing communications may completely miss some communications while copying and reviewing nearly 100% of others." *Id.* ¶ 19. In short, the interception, copying, and selector

[17] The calculation also "assumes a 0.00000001% chance" of the "NSA copying and reviewing any particular communication." Am. Compl. ¶ 58. But there is "no statistical foundation" for that assumption "in the Amended Complaint," and if the assumption is incorrect, then the conclusion could be "drastically affect[ed]" as a result. Salzberg Decl. ¶¶ 5, 11.

review of communications alleged by Plaintiffs is not random, as Wikimedia assumes in calculating the chances of intercepting its communications.

Thus, the Amended Complaint fails to substantiate and indeed contradicts a key assumption which, if incorrect, would invalidate the calculated odds of intercepting Wikimedia's communications. *Id.* ¶¶ 6, 14-15, 19-20. On the facts alleged in the Amended Complaint, "it is not statistically inconsistent for the NSA to have reviewed a very large number of communications but still have reviewed none" of Wikimedia's. *Id.* ¶ 8.

**4. Wikimedia's Allegation That the Geographic Distribution of its Communications Makes Interception of Those Communications a Virtual Certainty Also Rests on Unsupported Speculation About the Manner in Which Upstream Surveillance is Conducted.**

Wikimedia also cites the alleged geographic distribution of its communications, together with its assessment of how the NSA "must be" conducting Upstream collection to "reliably" achieve its objectives, as establishing a virtual certainty that its communications are intercepted as part of that program. *See* Am. Compl. ¶¶ 60–69. But Wikimedia's analysis is flawed. The operational details of Upstream collection remain classified, and Wikimedia's allegations regarding the manner in which Upstream surveillance "must be" conducted are based on technological misperceptions of how communications travel on the Internet. Thus, whether the NSA does or does not carry out Upstream surveillance in the manner Wikimedia describes remains a matter of speculation on par with that rejected by the Court in *Amnesty International*.

To establish that its communications "must" be collected as part of Upstream surveillance as an operational matter, Wikimedia first juxtaposes the alleged worldwide distribution of its communications with the limited number of locations at which Internet traffic might enter or exit the country. Plaintiffs allege that "almost all international [I]nternet traffic . . . flows" into or out of the United States at "chokepoints" where "approximately 49 international submarine cables" enter the country. Am. Compl. ¶ 60. Given the "relatively small number of international

chokepoints," Wikimedia claims that its "communications almost certainly traverse every [such] international backbone link." *Id.* ¶ 61. Wikimedia infers that if Upstream collection is occurring on any one of these links, it must be capturing Wikimedia's communications. *See id.* ¶¶ 60–61.

But Wikimedia's description oversimplifies—and assumes, incorrectly, that to intercept some communications carried on a backbone cable requires intercepting them all. While it may be accurate to say that the Internet "backbone" includes approximately 49 submarine cables on which international communications may travel, "[e]very such modern fiber-optic cable, in turn, consists of multiple smaller sub-cables housed inside that can each contain up to one thousand silica glass fibers." Lee Decl. ¶ 11. Importantly, "it would not be necessary, *as a technical matter*, to copy all the streams of communications on an entire backbone cable in order to copy all of the communications traveling across a particular sub-cable within that backbone cable."[18] *Id.* ¶ 13; *see also id.* ¶ 2. Thus, even if the NSA were copying and reviewing streams of electronic communications on a given backbone cable through which Wikimedia's communications passed, it does not necessarily follow that the NSA would be copying and reviewing all streams carried on that cable, or even the streams carried on the particular sub-cables through which Wikimedia's (or any of the Plaintiffs') communications passed. *See id.* ¶ 13. Wikimedia can only speculate whether that is the case, or not, which is insufficient for purposes of establishing its standing.

Nor does the fact that communications travel on the Internet in discrete "packets" compel the conclusion that the NSA intercepts, copies, and reviews for selectors all communications that transit a given backbone link. Wikimedia contends that because communications traverse the Internet in packets that "travel independently of one another," "the government must first copy

[18] Mr. Lee emphasizes that he "[has] no knowledge of how the NSA conducts the surveillance at issue in this case" but is providing this assessment "as a matter of technology." Lee Decl. at 7, n.5.

*all* such packets traversing a given backbone link" to "reliably" obtain the packets necessary to reconstruct any communications of interest. *Id.* ¶ 63. On this basis, Wikimedia concludes that, "even if the NSA conducts Upstream surveillance on only a single internet backbone link," it must be copying *all* communications flowing across that link, including Wikimedia's. *Id.* ¶ 64.

But Wikimedia overstates matters, at best. "Generally, all of the packets comprising a single communication travel on the same single hair-thin glass fiber" within a single sub-cable. Lee Decl. ¶ 12. "When information is broken into packets pursuant to the TCP/IP protocol[19] . . . it is possible, but unlikely, that routers will direct the packets to different paths." *Id.* "Typically, the packets of one communication will be separated and sent on different paths only if a change in conditions—such as a suddenly high volume of traffic on the initial path—renders a different path more advantageous than the route initially selected." *Id.* Thus, "[b]ecause the packets constituting a single communication are likely to travel on the same fiber within a sub-cable of a backbone cable, it would not be necessary, *as a technical matter*, to copy the entire stream of communications carried on every fiber within a sub-cable," *id.* ¶ 13, much less to copy the entire stream of communication carried on the larger backbone cable, to reliably obtain the packets comprising one communication.[20]

Finally, Wikimedia alleges that the NSA must be intercepting, copying, and reviewing all communications carried on "many different" backbone links because of its "strong incentive" to ensure that it has "reliably" and "comprehensively" obtained all communications associated with its targets. Am. Compl. ¶ 62, 64-66. But that is mere conjecture. Plaintiffs "have no actual

[19] "'Transport Control Protocol/Internet Protocol' ('TCP/IP') is "a set of rules or protocols" that "devices connected to the Internet follow." Lee Decl. ¶ 6. It "facilitates communication between different computers or networks of computers, and, among other things, it establishes rules for breaking communications into 'packets' that can travel efficiently." *Id.*

[20] Furthermore, "not all packets of a given TCP stream are necessary to intelligibly assemble its contents." *Id.* ¶ 13 n.4. Thus, it is not always necessary to collect every packet associated with a communication to reconstruct the contents of a TCP stream.

knowledge of the [NSA's] targeting practices," *Amnesty Int'l*, 133 S. Ct. at 1148-49. They have no idea how the NSA has defined the operational objectives of Upstream surveillance in practice, or the extent to which the NSA has committed its technical, financial, and personnel resources to the achievement of those objectives as opposed to providing operational support for other forms of surveillance it must also conduct to protect national security. Plaintiffs' speculation "as to how the [NSA] will exercise its discretion in determining which communications to target," and how, is insufficient to establish Wikimedia's standing. *Id.* at 1149.

Wikimedia's allegations regarding the manner in which it believes Upstream surveillance must be conducted touch on highly sensitive and classified operational details about the program. Any attempt on Plaintiffs' part to discover the truth of these matters (were this case to proceed beyond the pleading stage) would potentially implicate privileged state secrets. *See Jewel*, 2015 WL 545925, at *1, 5. For present purposes, however, it suffices to observe that Plaintiffs can only guess whether Upstream surveillance is carried out in any manner resembling their allegations. For this reason as well, the "virtual[ ] certain[ty]" that the NSA intercepts, copies, and reviews Wikimedia's communications for selectors amounts to nothing more than speculation, and will not suffice to establish Wikimedia's Article III standing.

**5. The Allegation that the Volume and Distribution of Wikimedia's Communications Make it Likely That They Have Been Intercepted, Copied, and Reviewed in the Upstream Process is Legally Insufficient, Under *Amnesty International*, to Establish Wikimedia's Standing.**

Wikimedia's standing arguments are not only factually unsubstantiated, they are foreclosed as a matter of law by Supreme Court precedent. In *Amnesty International*, the plaintiffs challenged the legality of Section 702 on the day it was enacted. *See* 133 S. Ct. at 1146. Lacking "any evidence that their communications ha[d] been monitored under" any program authorized by the statute, "a failure," the Court noted, that "substantially undermine[d] their standing theory," *id.* at 1148, the plaintiffs claimed instead that they had standing because

there was an "objectively reasonable likelihood" that their communications "[would] be intercepted" "in the future." *Id.* at 1147.

The Supreme Court rejected this "novel view of standing," *id.* at 1146, because it was "inconsistent with [its] requirement that the threatened injury must be certainly impending to constitute injury in fact." *Id.* at 1147. In so holding, the majority declined to follow the approach advocated by the dissenting Justices, who, relying on "commonsense inferences," found a "very high likelihood" that the Government would "intercept at least some of the" plaintiffs' communications. *Id.* at 1157 (Breyer, J., dissenting). The dissent relied on a combination of facts, including (1) that the plaintiffs regularly engaged in the type of electronic communications—with and about suspected foreign terrorists, their families and associates, and their activities—that the Government had "the capacity" to collect and was highly "motivated," for counter-terrorism purposes, to intercept, and (2) that the Government had in fact intercepted such communications on thousands of occasions in the past. *Id.* at 1156–59.

Like the plaintiffs in *Amnesty International*, Wikimedia "fail[s] to offer" any well-pled allegations "that [its] communications have been monitored under" Upstream, *id.* at 1148, and instead it tacitly advances a "likelihood" theory of standing —oversold as a "virtual[] certain[ty]," Am. Compl. ¶ 58—that is remarkably similar to the one rejected in *Amnesty International*. Wikimedia would have the Court infer that the NSA intercepts its communications—without any allegations of specific facts demonstrating that to be so—based on generalized allegations about the volume and distribution of its communications, and uninformed speculation about how the NSA "must be" conducting Upstream surveillance that rests on assumptions (of the very kind rejected by the majority in *Amnesty International*) about the NSA's motives and capabilities. *See id.* ¶¶ 57-67.

The Court should reject this repackaged theory of standing. *Amnesty International* teaches that relying solely on supposedly "commonsense inferences," *id.* at 1157 (Breyer, J., dissenting), based on limited knowledge—or, more accurately, "mere[ ] speculat[ion]," without any "actual knowledge," *id.* at 1148—about the scope and operation of the Government's classified intelligence-gathering activities, is not a sufficiently "rigorous" basis on which to find standing to challenge those activities. *See id*. at 1147. Rather, at a minimum, the Amended Complaint must adequately plead facts plausibly demonstrating that Wikimedia's communications have been or imminently will be intercepted under the program. *See id.* at 1149; *Iqbal*, 556 U.S. at 678–79; *David*, 704 F.3d at 333; *Zander*, 786 F. Supp. 2d at 883. As discussed above, Wikimedia has made no such specific allegations.

### C. Wikimedia Has Alleged No Injury from the Claimed Interception, Copying and Review of Its Online Communications.

Even if Wikimedia plausibly alleged a likelihood that the NSA intercepts, copies, and reviews for selectors Wikimedia's "communications with its community members" and the logs thereof, Am. Compl. ¶ 86, and even if that alleged likelihood were sufficient, under *Amnesty International*, to confer Article III standing, Wikimedia would still lack prudential standing to challenge the alleged interception, copying, and review of these communications. This is so because Wikimedia lacks third-party standing to raise the legal rights and interests of these unidentified Internet users who view, contribute to or otherwise interact online with its websites.

As discussed above, by "communications with its community members" Wikimedia principally means Internet users visiting its web pages, to read or sometimes edit their content, or to communicate with one another through a Wikimedia website. *Id.* ¶¶ 81, 86. To communicate on the Internet, whether to send and receive e-mail, "browse" the World Wide Web, or otherwise, a user must obtain a connection from an Internet service provider ("ISP"). Lee Decl.

¶ 5.[21] When a user, by means of a computer or other device, makes a request to view or download information located on a website, the ISP through which the user accesses the Internet at that particular time and place assigns a public Internet Protocol ("IP") address to communications associated with the user's device. *Id.* ¶¶ 9, 15.[22] The global communications network then routes the user's request, together with the assigned public IP address, to the public IP address of the computers on which the website is housed. *Id.* ¶ 16. Upon receiving the request, the website's host computers automatically generate and send one or more return messages that include the information requested by the user (usually broken down into packets) and the public IP address previously assigned to the user's request, which the global network then uses to route the response (via the ISP) to the user's device. *Id.* ¶ 17; *see id.* ¶¶ 6-7.

At no time during this automated process do the website's operators learn the identity of the user (unless the user him or herself has conveyed that information to the website). *Id.* ¶ 10. The request is identified by the public IP address associated with it; the ISP may (or may not) know the identity of the user who made the request, but the website does not. *Id.* Furthermore, the IP address associated with future requests by the same user may change, depending on when and where the user makes those future requests. *Id.* ¶ 21.[23]

---

[21] Users may connect, for example, at home through service to which they personally subscribe; at work, through their employer's ISP; or through an ISP furnishing service to a public establishment such as an "Internet café" or a Starbucks. Lee Decl. ¶ 21a–e.

[22] The IP address may be static (permanent), as some ISPs assign to home subscribers, or a dynamic (temporary) IP address that may change after a period of time, such as an hour, a day, or the duration of the user's Internet session, depending on the ISP's practices. Lee Decl. ¶ 15.

[23] For example, a request sent from an individual's home will be associated with an IP address that was assigned by the ISP to whose service the homeowner subscribes, but the user could be the homeowner, or a family member, using the homeowner's personal computer, or a visitor using his or her own laptop computer who connects through the homeowner's Wi-Fi network. Lee Decl. ¶ 21.a. A request made by a user at his or her place of employment, using an employer-provided desktop computer, will be associated with a public IP address assigned by the employer's ISP, which may be assigned the next day, hour, or even moment to the online communications of other individuals working for the same employer. *Id.* ¶ 21.b.

In short, what Plaintiff Wikimedia calls "communications with its community members," Am. Compl. ¶ 86, are nothing more than automated transmissions of publicly available information displayed on its websites, transmissions made at the initiation of anonymous electronic requests identified by IP addresses. The information is not created by Wikimedia but supplied by other, typically anonymous third parties, *see id.* ¶¶ 79–80; Wikimedia provides only the "technical infrastructure" needed to post it on the World Wide Web, *id.* ¶ 82.[24] The content is not privately held but made publicly available on Wikimedia websites for the use, education, and enjoyment of anyone in the world—Wikimedia's self-stated raison d'être. *Id.* ¶¶ 6, 78.[25] These transmissions are not initiated by Wikimedia nor does any living being employed by Wikimedia select their contents. Rather, they are the mechanized responses of Wikimedia computers to electronic requests received from digital devices belonging to individual Internet users, who designate the content they wish to receive. Lee Decl. ¶¶ 17, 19.

Nor does Wikimedia know (or care, *see* Am. Compl. ¶ 78) to whom it sends the information. It knows only the IP addresses associated with the communications in which these requests are received. Lee Decl. ¶¶ 16-20. It knows nothing about the actual identities of the

[24] As stated in the overview to Wikimedia's own Terms of Use for contributors, authors, and editors, http://wikimediafoundation.org/wiki/Terms_of_Use (last visited on August 5, 2015), Wikimedia does not "contribute, monitor, or delete content" on its websites, it "merely host[s] this content," "maintaining the infrastructure and organizational framework that allows [its] users to build the Wikimedia [websites] by contributing and editing [the] content themselves." *See also id.* ("Our Services") (Wikimedia "do[es] not take an editorial role" but "simply provide[s] access to the content that . . . users have contributed and edited.").

[25] *See Maryland v. Macon*, 472 U.S. 463, 469 (1985) (undercover officer did not infringe on a legitimate expectation of privacy by entering bookstore and examining books "that were intentionally exposed to all who frequent[ed] the place of business") (citing *Katz v. United States*, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.")); *see also United States v. Baalerud*, 2015 WL 1349821, at *8 (W.D.N.C. Mar. 25, 2015) (noting that every court of appeals to consider the question has held that there is no reasonable expectation of privacy in personal computer files that are made publicly available through use of peer-to-peer software) (citing cases).

users who view or download contents from its websites unless those users specifically provide that information to the websites. *Id.* ¶¶ 19-21.

It comes as little surprise, therefore, that the Amended Complaint identifies no privacy interest *of Wikimedia's* in these "communications with its community members," or in Wikimedia's internal "log[s]" of the communications. *Id.* ¶ 86. Rather, it speaks only in terms of *users'* privacy interests. According to the Amended Complaint, "Wikimedia's communications with its community members, as well as its internal [log] communications . . . are often sensitive and private," because they "reveal a detailed picture of the everyday concerns and reading habits of Wikimedia's users, and often constitute a record of their political, religious, sexual, medical, and expressive interests." *Id.* ¶ 95.[26] Thus, even if Wikimedia adequately alleged NSA interception, copying and selector review of these communications, the Amended Complaint alleges no resulting injury except (arguably) to the privacy of online users. [27]

Wikimedia lacks standing, however, to assert the privacy rights of unidentified Internet users who happen to view, download, or even edit information on its websites. Prudential limits on standing generally bar litigants from basing their claims on the legal rights and interests of third parties not before the court. *Tesmer*, 543 U.S. at 129; *Doe*, 713 F.3d at 754. The rule against third-party standing may be overcome only where a plaintiff "demonstrate[s]: (1) an

[26] *See also id.* ¶¶ 89-94. (alleging that online communications with Wikimedia websites reveal what users read or write on, or the information they request from, Wikimedia websites, as well as other information about them including IP addresses, their user names and other log-in credentials, the type of devices they use online, and their approximate geographic location); *id.* ¶¶ 93-94 (alleging that Wikimedia's internal log communications contain similar information about online users who view, contribute to or otherwise communicate via Wikimedia websites).

[27] Wikimedia also alleges no privacy interest of its own in the communications through which its users "interact" with one another. The Amended Complaint describes these communications as including e-mail among registered users of Wikimedia accounts, restricted-access wikis (collaborative web pages), and user mailing lists. Am. Compl. ¶ 92. Although Wikimedia allegedly supplies the technical infrastructure to make these user-to-user communications possible, *see id.*¶ 82 (much like a typical Internet service provider), Wikimedia identifies no privacy interest it possesses in these communications between and among users.

injury-in-fact; (2) a close relationship between [itself] and the person[s] whose right[s] [it] seeks to assert; and (3) a hindrance to the third part[ies'] ability to protect [their] interests." *Freilich*, 313 F.3d at 215 (citation omitted). Wikimedia satisfies none of these requirements so far as transmissions between its websites and anonymous users, and its logs thereof, are concerned.

First, as discussed *supra*, at 39, the Amended Complaint does not even purport to identify an injury to Wikimedia's privacy interests from the alleged NSA interception, copying, and selector review of transmissions between Wikimedia websites and Internet users. *See generally* Am. Compl. ¶¶ 78–109.[28] Second, the Amended Complaint does not plausibly allege a "close relationship" between Wikimedia and the alleged hundreds of millions of anonymous visitors to its websites, *id.* ¶¶ 2, 79, ordinary persons, browsing the Internet, whose identities are entirely unknown to it, *see supra*, at 38. *Cf. Tesmer*, 543 U.S. at 130–31 (attorneys seeking to challenge constitutionality of state law restricting appointment of appellate counsel for indigent defendants did not have a "close relationship" with "as yet unascertained . . . criminal defendants").

Third, even if Wikimedia met these first two requirements, it has not alleged a hindrance to users' ability to bring suits such as this on their own. Wikimedia suggests that the rights of its "community members" will be impaired if it is not permitted to maintain this suit, because they "are so numerous, because they are dispersed across the globe, and because millions of them choose to interact with Wikimedia anonymously." Am. Compl. ¶ 111. But the numerosity of

[28] Wikimedia alleges in passing that its communications "also reveal private information about its operations, including details about its technical infrastructure, its data flows, and its member community writ large." Am. Compl. ¶ 99. Even to begin to glean such information, however, would require more than simply intercepting, copying, and reviewing online communications for targeted selectors. "[S]ubstantially all of the traffic flowing to and from [a] website's servers . . .would need to be recorded, ingested into a database, and then . . . analyzed to try to piece together the infrastructure and data flows involved." Lee Decl. ¶ 8 n.3. As discussed in § III, *infra*, none of the Plaintiffs, including Wikimedia, has plausibly alleged that any of their online communications are actually retained and reviewed in NSA databases. Thus the Amended Complaint alleges no infringement on the privacy interest asserted in paragraph 99 that could support Wikimedia's standing.

Wikimedia's "community members" (allegedly hundreds of millions) makes it far more likely, not less, that willing and able plaintiffs can be found among them. *See American Immigration Lawyers Ass'n v. Reno*, 199 F.3d 1352, 1363 (D.C. Cir. 2000) (denying third-party standing to immigrant rights organization where approximately 10,000 potential plaintiffs were available to contest allegedly unlawful removal procedures). And courts have rejected the proposition that overseas aliens, as such, face such insuperable barriers to suit in the United States that third parties must be permitted to assert their rights, especially where organizations such as Plaintiffs here (and their counsel) are in a position to provide legal assistance to potential plaintiffs. *See American Immigration Lawyers Ass'n*, 199 F.3d at 1362-63; *Fenstermaker v. Bush*, 2007 WL 1705068 *5 & n.6 (S.D.N.Y. June 12, 2007).[29]

The anonymity of typical users' interactions with Wikimedia's websites is not a matter of conscious choice, as Plaintiffs suggest, but the default condition when users view or download information available on a Wikimedia website, or any of the millions of other sites found on the World Wide Web. Lee Decl. ¶¶ 19-21. Revealing that one uses the Internet hardly amounts to the kind of privacy concern that has been recognized as a deterrent to rightholders' defense of their own interests. *See Carey v. Population Servs. Int'l*, 431 U.S. 678, 684 n.4 (1977) (vendor had third-party standing to challenge law restricting sale of contraceptives to minors because potential purchasers may be chilled from asserting their own rights by a desire to protect their privacy) (citing *Singleton v. Wulff*, 428 U.S. 106, 117 (1976) (plurality opinion) (physicians may assert rights of patients to obtain abortions because desire to protect the privacy of their decision

[29] If Plaintiffs' objective in this case is to litigate whether Upstream surveillance violates the Fourth Amendment rights of non-U.S. persons located outside the United States who use the Internet, then—*if* Plaintiffs had standing—this case could be easily decided. The protections of the Fourth Amendment do not extend to non-U.S. persons located abroad. *United States v. Verdugo-Urquidez*, 494 U.S. 259, 264-67 (1990); *see United States v. Mohamud*, 2014 WL 2866749 *13 (D. Or. June 24, 2014). Moreover, as the Supreme Court has often held, Fourth Amendment rights are personal rights that cannot be asserted vicariously. *Rakas v. Illinois*, 439 U.S. 128, 140 (1978); *California Bankers Ass'n v. Schultz*, 416 U.S. 21, 69-70 n.8 (1974).

may prevent patients from filing suit)); *see also Miller v. Albright*, 523 U.S. 420, 449 (1998) (O'Connor, J., concurring). Indeed, the presence of eight other plaintiffs to this suit alone, and the multiple plaintiffs who challenged Upstream collection in *Jewel*, 2015 WL 545925, at *1–2, belies any sweeping claim that Internet users as a class face obstacles that deter them from mounting legal challenges to Upstream surveillance.

In short, Plaintiffs have not plausibly alleged injuries to themselves that are sufficient under *Amnesty International* to confer standing to contest the legality of alleged NSA interception, copying, and selector review of international online communications during the Upstream collection process.

## III. PLAINTIFFS HAVE NOT PLAUSIBLY ALLEGED THAT COMMUNICATIONS OF THEIRS ARE RETAINED, READ, AND DISSEMINATED BY THE NSA AS PART OF THE UPSTREAM SURVEILLANCE PROCESS.

Because Plaintiffs do not plausibly allege initial NSA interception, copying, and selector review of their online communications, it necessarily follows that they have not adequately alleged that any of their communications are retained, read, or disseminated by the NSA, and the standing inquiry should end there. But even if they had adequately pled interception, copying, and review, Plaintiffs would still fail to establish their standing to challenge the subsequent alleged retention, analysis, and dissemination of their communications, for precisely the same reasons that the plaintiffs failed to establish their Article III standing in *Amnesty International*.

### A. Plaintiffs' Allegations That Their Staffs Engage in Communications With Likely Targets of Upstream Surveillance, About Topics That Could Be Considered Foreign-Intelligence Information, Are Insufficient Under *Amnesty International* to Establish Their Standing.

Plaintiffs allege that they communicate with people "whom the government is likely to target when conducting Upstream surveillance," such as foreign government officials, journalists, experts, human rights defenders, victims of human rights abuses, and others believed to have information relevant to counterterrorism efforts, and that "[a] significant amount of the

information that Plaintiffs exchange over the internet is 'foreign intelligence information' within the meaning of the FAA." Am. Compl. ¶¶ 73–74; *see also id.* ¶¶ 104, 105, 115, 125, 126, 133, 138, 143, 148, 153, 158, 163. Plaintiffs do not claim to communicate with particular individuals whom the Government has acknowledged as targets of Upstream surveillance. Indeed, the Government has not publicly disclosed whom it targets under the program, or the particular categories of foreign-intelligence information that it is authorized to acquire. *See* PCLOB Report at 24-25 & n.70 (noting that the Government's Section 702 certifications, *see supra*, at 7-8, "identify categories of foreign intelligence information" whose acquisition is authorized). Rather, Plaintiffs surmise that "because of the nature of their communications, and the location and identities of the individuals and groups with whom and about whom they communicate, there is a substantial likelihood that Plaintiffs' communications intercepted by the NSA through Upstream surveillance are retained, read, and disseminated." Am. Compl. ¶ 71.

These allegations are nearly identical, however, to the allegations the Supreme Court rejected as too speculative in *Amnesty International*. *See* 133 S. Ct. at 1148–50. There, the plaintiffs alleged that "[b]ecause of the nature of their communications and the identities and geographic location of the individuals with whom they communicate, plaintiffs reasonably believe that their communications will be acquired, analyzed, retained, and disseminated under the challenged law." *See, e.g.*, *Amnesty Int'l, USA v. Clapper*, No. 08-cv-6259 (S.D.N.Y.), Pls. Mot. for Summ. Judg. at 11 (Exh. 4, hereto). While the plaintiffs in *Amnesty International* asserted that they "*reasonably believe[d]* that their communications [would] be acquired, analyzed, retained, and disseminated under [Section 702]," *id.* (emphasis added), Plaintiffs here allege a "*substantial likelihood* that Plaintiffs' communications intercepted by the NSA through Upstream surveillance are retained, read, and disseminated." Am. Compl. ¶ 71 (emphasis added). But regardless of whether Plaintiffs purport to hold a "reasonable belief" or assert a

"substantial likelihood" of retention, the result is the same: the Supreme Court explicitly rejected the notion that an "objectively reasonable likelihood" standard is consistent with the "requirement that threatened injury must be certainly impending to constitute injury in fact." *Amnesty Int'l*, 133 S. Ct. at 1147 (citation omitted).

Consequently, Plaintiffs' assertion here, like the one made by the plaintiffs in *Amnesty International*, that the Government "will target . . . [plaintiffs'] foreign contacts," *id.* at 1148, is "necessarily conjectural," because Plaintiffs have "no actual knowledge of the Government's" "targeting practices," *id.* at 1148–49. Instead of adequately pleading facts "demonstrating that the communications of their foreign contacts will be targeted," *id.* at 1148–49, Plaintiffs "merely speculate and make assumptions about whether their communications with their foreign contacts will be acquired under [Section 702]." *Id.* at 1148. This is insufficient to confer standing.[30]

Moreover, even if Plaintiffs had plausibly alleged that their foreign contacts' or their own communications were retained, they would still need to show that their injury is fairly traceable to Upstream surveillance. *See id.* at 1147. Because Plaintiffs can only speculate whether any asserted acquisition occurred via Upstream collection as opposed to PRISM, some other authority under FISA, or Executive Order 12333, they cannot demonstrate that their injury is "fairly traceable" to the Government conduct they seek to challenge. *See id.* at 1149.

**B. NACDL Has Not Established Its Standing to Sue on Behalf of its Members.**

In contrast to the other eight Plaintiffs, NACDL alleges the retention, analysis and dissemination of its individual members' communications, and purports to sue on their behalf.

[30] Indeed, Plaintiffs' allegations here often contain less specificity than the declarations found wanting in *Amnesty International*. *Compare* Am. Compl. ¶¶ 130–134 (describing in general terms the types of foreign individuals and entities with whom Human Rights Watch ("HRW") communicates about "topics that fall within the FAA's expansive definition of 'foreign intelligence information'"), *with* Mariner Decl. ¶¶ 4–9 (filed in *Amnesty International)* (attached as Exh. 5, hereto) (identifying particular individuals with whom an HRW Program Director communicates abroad, such as HRW's Pakistan researcher based in Europe, and specifying putative subjects of foreign-intelligence information, such as the CIA rendition program).

Am. Compl. ¶¶ 7, 115–16. NACDL asserts that its members' communications are likely retained by the NSA because they engage in communications with or about "likely targets" of Upstream surveillance regarding topics that could be considered foreign-intelligence information. *Id.* ¶ 115. It also contends that the communications of defense attorneys in prosecutions where the Government has acknowledged use of FAA surveillance are "especially likely" to be retained as part of the Upstream collection process, *id*. ¶ 116, and identifies one of its members, Joshua L. Dratel, as one such attorney whose communications are "especially likely" to be retained by the NSA, *id.* ¶ 127. As discussed in § III.A, above, such speculative assertions are insufficient for purposes of establishing that any of NACDL's members, including Mr. Dratel, have suffered injury traceable to Upstream surveillance. *Amnesty Int'l*, 133 S. Ct. at 1149. Thus, NACDL fails to establish its associational standing to sue on its members' behalf.

An organization "can assert standing . . . as a representative of its members" if: "(1) its own members would have standing to sue in their own right; (2) the interests the organization seeks to protect are germane to the organization's purpose; and (3) neither the claim nor the relief sought requires the participation of individual members in the lawsuit." *Southern Walk*, 713 F.3d at 182, 183–84 (citations omitted). Regarding the first prong of this test, "[t]he Supreme Court has clarified that to show that its members would have standing, an organization must 'make specific allegations establishing that at least one *identified member* ha[s] suffered or [will] suffer harm.'" *Id.* at 184 (quoting *Summers*, 555 U.S. at 498 (emphasis by the Court of Appeals)). This aspect of the test is grounded in "the constitutional requirement of a case or controversy," *United Food & Commercial Workers v. Brown Group, Inc.*, 517 U.S. 544, 554–55 (1996), and is thus "an Article III necessity for an association's representative suit," *id.* at 555.

In accordance with that requirement, the Supreme Court in *Summers* specifically rejected a theory of representational standing based on "a statistical probability that some of [an

organization's] members are threatened with concrete injury." 555 U.S. at 497. In particular, the Court held that an uncontested showing that "it [was] possible—perhaps even likely—that one individual [would] meet all of [the] criteria" for standing "[did] not suffice." *Id.* at 499.

Yet that is the very approach NACDL urges here. NACDL alleges only "*a substantial likelihood* that the NSA retains, reads, and disseminates international communications of NACDL's members," Am. Compl. ¶ at 115 (emphasis added), and refers to a group of members, including Mr. Dratel, that it claims "*is especially likely* to have [its] communications retained, read, and disseminated in the course of Upstream surveillance," *id.* ¶ 116 (emphasis added); *see also id.* ¶ 127. Claiming organizational standing on the basis of such allegations is contrary to the Supreme Court's express instructions in *Summers*: even if it is "likely" that some member will meet the criteria for standing, "that speculation does not suffice," 555 U.S. at 499; an organization must identify specific members "who have suffered the requisite harm." *Id.*

Moreover, in support of its claim generally that its members' communications are retained by the NSA as part of the Upstream process, NACDL relies on assertions regarding its members' communications with "likely targets" of surveillance about subjects that could be considered foreign-intelligence information, Am. Compl. ¶ 115, allegations that, as discussed in § III.A, above, were rejected as inadequate in *Amnesty International.* For this reason, as well, NACDL's allegations are insufficient to establish its members' standing, and therefore its own.

NACDL next contends that the communications of a particular group of its members, defense attorneys (including Mr. Dratel) "who represent individuals in criminal prosecutions in which the government has acknowledged its use [of] FAA surveillance," are "especially likely" to be retained by the NSA as part of the Upstream collection process. Am. Compl. ¶ 116. But this asserted basis for the standing of NACDL's members likewise rests on a "speculative chain of possibilities," 133 S. Ct. at 1150, similar to that rejected in *Amnesty International*.

To begin with, "FAA surveillance" is not synonymous with Upstream collection. Rather, under Section 702 of the FAA, the NSA may use two different means to acquire a target's electronic communications, either Upstream collection of communications as they transit the Internet "backbone," or the acquisition of communications directly from U.S.-based providers as part of its PRISM collection. *See supra*, at 10. Indeed, in a 2011 opinion, the FISC observed that the "vast majority of communications" acquired pursuant to Section 702, more than 90 percent, were acquired using PRISM collection, rather than Upstream. Oct. 3, 2011 FISC Op. at 29-30. Thus, in any case where the Government provided notice of use of FAA-derived information, the information may have been acquired through PRISM or Upstream, yet to establish its standing, NACDL "would . . . need to show that [its members'] injury is fairly traceable to [the surveillance program that it challenges here]. But, because [NACDL and its members] can only speculate as to whether any (asserted) interception [was] under [Upstream] or [PRISM], they cannot satisfy the 'fairly traceable' requirement." *Id.*

Additionally, just as in *Amnesty International*, Plaintiffs here "have no actual knowledge of the Government's . . . targeting practices" employed in Upstream surveillance, 133 S. Ct. at 1148, and thus can "merely speculate and make assumptions about whether their communications with their foreign contacts will be acquired" under the program they challenge. *Id*. Contrary to Plaintiffs' allegations that the targeted selectors "in several of these cases" have been identified in press reports or other publicly-available documents, *see* Am. Compl. ¶ 116, the Government's targeting practices employed in Upstream surveillance remain classified. Without true knowledge regarding the targets of the Government's surveillance, NACDL and its members can only speculate that they communicated with or about a target such that their communications would have been acquired. Likewise, NACDL and its members can only

speculate that an individual who was a target of surveillance at one time remained a target by the time defense counsel began working on the case in which that individual was involved.

All the same is true regarding Mr. Dratel, on whom NACDL focuses in an apparent effort to satisfy the requirement of identifying at least one of its members who has suffered injury in fact. *See Summers*, 555 U.S. at 498. Although the claims regarding the alleged surveillance of his communications are emphatic, *see* Am. Compl. ¶ 127, at bottom, they are no different from the speculative claims discussed above. Just like NACDL's other members, Mr. Dratel can only guess at whether the particular individuals with whom he communicates are targets of surveillance at all, much less Upstream surveillance. Because the allegations about Mr. Dratel fail to establish that he has standing in his own right, they fail to establish NACDL's organizational standing as well. *Summers*, 555 U.S. at 498.

The Amended Complaint refers to a client of Mr. Dratel's "who has received notice of FAA surveillance." *Id.* ¶ 121. Defendants have identified two cases to which this allegation may refer: *Unites States v. Mohamud*, and *United States v. Hasbajrami*.[31] In neither case did the Government indicate whether the information at issue was derived from Upstream or PRISM collection.[32] Additionally, contrary to Plaintiffs' suggestion that targeted selectors were disclosed in these cases, *see* Am. Compl. ¶ 116, the Government has not declassified any of the targeting procedures or selectors in question, or even whether the defendants were the targets of the surveillance or merely subjects of incidental collection. (In any event, NACDL fails to

[31] *See* Government's Supplemental FISA Notification, *Unites States v. Mohamud*, 3:10-cr-00475 (D. Or.), ECF No. 486 (Nov. 19, 2013) (Exh. 6, hereto) ("*Mohamud* Notice"); Letter re Supplemental Notification, *United States v. Hasbajrami*, 1:11-cr-00623 (E.D.NY.), ECF No. 65 (Feb. 24, 2014) (Exh. 7, hereto) ("*Hasbajrami* Notice").

[32] Indeed, in *Hasbajrami*, counsel for Plaintiffs here wrote, as *amicus curiae*: "the government conducts two types of surveillance under the FAA: PRISM surveillance and Upstream surveillance . . . . The government has not disclosed which specific program or programs it relied upon in this case." Brief of *Amici Curiae* [ACLU] and Electronic Frontier Found. in Supp. of Def.'s Mot. to Suppress, 11-cr-00623, ECF No 94-1 (Exh. 8, hereto) at 7.

explain how the alleged identification of the selectors reveals whether Upstream or PRISM collection was employed.) The notices at issue also provide no information regarding the nature of the FAA-derived information. *See Mohamud* Notice at 1–2; *Hasbajrami* Notice at 1–2. There is simply no non-speculative basis on which to conclude that Mr. Dratel (or any other particular individual) was subject to Upstream surveillance based on his involvement in these proceedings.

Plaintiffs also aver that Mr. Dratel previously represented a client "where officials have told Congress that the government used FAA surveillance in the course of its investigation." Am. Compl. ¶ 121. Plaintiffs appears to be referring to *Hasanoff v. United States* and the Congressional testimony given by Sean Joyce, then-Deputy Director of the FBI, regarding FAA-obtained communications between an extremist in Yemen and a person in the United States, *other* than Mr. Dratel's client, Mr. Hasanoff. *See* Mem. of Law, *Hasanoff v. United States*, 10 Cr. 162 (S.D.N.Y.), ECF No. 208 (Exh. 9, hereto) at 10–11. Nothing in that testimony suggests that either Mr. Dratel, or his client, Mr. Hasanoff, were subject to FAA surveillance. *See id.*[33]

In sum, Plaintiffs' allegations do not establish that any member of NACDL—including Mr. Dratel—has sustained an injury that is "fairly traceable to" Upstream surveillance. 133 S. Ct. at 1150. Under *Amnesty International* and *Summers*, this Court should reject NACDL's assertion of representational standing.

## IV. PLAINTIFFS' ALLEGATIONS THAT UPSTREAM COLLECTION "UNDERMINES [THEIR] ABILITY TO CONDUCT [THEIR] WORK" ALSO FAIL TO ESTABLISH AN INJURY SUFFICIENT TO CONFER STANDING.

Plaintiffs' and Mr. Dratel's claims that Upstream collection inhibits their ability to conduct their work are also inadequate under *Amnesty International* to establish standing. The

[33] The Amended Complaint refers to three other clients of Mr. Dratel, Wadith El Hage, David Hicks, and Baasaly Moalin, but NACDL does not allege that any of those individuals were subject to Upstream or even FAA surveillance. Am. Compl. ¶ 120. Indeed, in Mr. Moalin's case, the Government acknowledged using a different provision of FISA (50 U.S.C. § 1861) to obtain business records containing telephony metadata, not FAA surveillance. *See United States v. Moalin*, 2013 WL 6079518, at *5 (S.D. Cal. Nov. 18, 2013).

injuries Plaintiffs claim to suffer as a result of Upstream collection—the adoption of costly measures to minimize the risk of surveillance and the reduced likelihood that third parties will share sensitive information with them for fear of surveillance—arise from speculation as to how Upstream collection operates as well as the subjectively held, unsubstantiated fears of third parties. Such injuries are not fairly traceable to Upstream collection for Article III purposes.

Plaintiffs and Mr. Dratel first allege that Upstream collection injures them because it requires them to adopt taxing measures to reduce the risk that their communications will be acquired. To this end, Plaintiffs allege that they "have had to take burdensome and sometimes costly measures to minimize the chance that the confidentiality of their sensitive information will be compromised," such as developing new protocols for transmitting information, traveling long distances to collect information, and in some circumstances forgoing particularly sensitive communications altogether. *See* Am. Compl. ¶¶ 75, 128. As a result, Plaintiffs and Mr. Dratel emphasize that they are unable to gather and relay information, represent their clients, and engage in domestic and international advocacy as they would in the absence of the feared surveillance. *See id.* ¶ 76; *see also id.* ¶¶ 108, 109, 118, 128, 129, 134, 139, 144, 149, 154, 159, 164. Remarkably, Plaintiffs, which allegedly communicate with people in repressive countries that would seek to punish or retaliate against them for their activities, claim that it is the possibility of surveillance by the *United States* that has led them to take expensive precautions against the interception of their communications.[34] But even accepting these allegations at face value, they are insufficient, under *Amnesty International,* to confer standing.

[34] To be precise, Plaintiffs allege that they have taken these burdensome precautions only "in part [due] to NSA surveillance, including Upstream surveillance," Am. Compl. ¶¶ 109, 118, 128, 134, 139, 144, 149, 154, 159, 164, thus acknowledging that there are other reasons why they have taken these precautions, and raising the question whether this alleged injury is redressable by enjoining alleged Upstream surveillance of their communications.

In *Amnesty International*, the plaintiffs advanced and the Supreme Court rejected essentially indistinguishable arguments. *See* 133. S. Ct. at 1150–51 ("[Plaintiffs] assert that they are suffering ongoing injuries . . . because the risk of surveillance under § 1881a requires them to take costly and burdensome measures to protect the confidentiality of their communications."). In dismissing these arguments, the Court explained that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Id.* at 1151. Thus, "[a]ny ongoing injuries that [plaintiffs] are suffering are not fairly traceable to [Section 702]." *Id.*

The Court's reasoning applies directly to Plaintiffs' and Mr. Dratel's claims regarding Upstream collection. Their alleged adoption of costly measures to minimize the chance of their communications being acquired by Upstream collection is a self-inflicted injury based on a purely speculative threat. *See id.* at 1151–52. Because "the costs that they have incurred to avoid" such scrutiny "are simply the product of their fear of surveillance," any resulting injures are "insufficient to create standing." *Id.* at 1152. Indeed, "[i]f the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear." *Id.* at 1151. Thus, *Amnesty International* compels the conclusion that voluntary expenditures motivated by fears of hypothetical surveillance are an insufficient basis for Article III standing.

Plaintiffs and Mr. Dratel next allege that "ongoing government surveillance, including Upstream surveillance," inhibits their ability to conduct their work because it "reduces the likelihood that clients, users, journalists, witnesses, experts, civil society organizations, foreign government officials, victims of human rights abuses, and other individuals will share sensitive information with Plaintiffs." Am. Compl. ¶ 76; *see also id.* ¶¶ 89, 98, 108, 109, 110, 118, 128, 129, 134, 139, 144, 149, 154, 159, 164. The Court in *Amnesty International* disposed of the

precise claim that "third parties might be disinclined to speak with [the plaintiffs] due to a fear of surveillance" as insufficient to confer standing. 133 S. Ct. at 1152 n.7. In so doing, the Court reasoned that even if such an assertion were factual, it would "not establish an injury that [was] fairly traceable" to the challenged statute, because it was "based on third parties' subjective fear of surveillance." *Id.* (citing *Laird v. Tatum*, 408 US. 1, 10–14 (1972)).

The Court's reasoning in *Amnesty International* controls here. Hypothetical assertions of a "chill" upon the willingness of third parties to communicate with Plaintiffs or Mr. Dratel "do not establish injury that is fairly traceable to" Upstream collection "because they are based on third parties' subjective fear of surveillance," and not on the actual operation of the program. *Id.* at 1152 n.7. And, Plaintiffs' mere allegation of a "reduced likelihood" that third parties will share information with them is insufficient to plausibly establish that such harm is occurring in the first place. The Amended Complaint contains no factual support for Plaintiffs' and Mr. Dratel's conjecture that their third-party contacts have in fact declined or are reluctant to communicate with them because of Upstream collection. As the Supreme Court explained, "[a]llegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm." *Id.* at 1152 (citing *Laird*, 408 U.S. at 13–14). Thus, the subjective fears of third parties and any alleged accompanying consequences upon Plaintiffs do not establish Plaintiffs' standing.

## CONCLUSION

For all the foregoing reasons, the Plaintiffs' claims should be dismissed for lack of subject-matter jurisdiction.

Dated: August 6, 2015

Respectfully submitted,

BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Deputy Branch Director
JAMES J. GILLIGAN
Special Litigation Counsel

*/s/ James J. Gilligan*
RODNEY PATTON
JULIA A. BERMAN
CAROLINE J. ANDERSON
Trial Attorneys
U.S Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 6102
Washington, D.C. 20044
Phone: (202) 514-3358
Fax: (202) 616-8470
james.gilligan@usdoj.gov

Counsel for Defendants