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

Date: May 29, 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 7320
Washington, D.C. 20044
Phone: (202) 305-7919
Fax: (202) 616-8470
E-mail: rodney.patton@usdoj.gov

Counsel for Defendants

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

CASES **PAGE(S)**

STATUTES

LEGISLATIVE MATERIAL

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 nation's adversaries in order to detect and thwart threats against our nation and its people.

Specifically, Plaintiffs seek to contest the legality of the NSA's "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 (that is, 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 its 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 First and Fourth Amendments and Article III of the Constitution, and should be permanently enjoined. Plaintiffs have not established their standing, however, to assert any of these claims, and their claims, therefore, should be dismissed.

Although the technical operational details of Upstream surveillance remain classified, Plaintiffs posit that it involves an initial stage at which the NSA intercepts, copies, and 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 further review and 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 plaintiff organizations] [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 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 entirely on their conclusory assertion that the NSA intercepts, copies, and reviews *substantially all* international online communications carried in the United States. But the Complaint contains no factual enhancement to support this allegation, and therefore, 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' 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.

Plaintiff Wikimedia Foundation attempts to avoid this conclusion in its case with the allegation that it engages every month in tens of billions of Internet communications "related to the activities of its users"—by which it principally means requests to view and download information from its public websites made by anonymous users of the Internet. The inference the Court is meant to draw from this allegation, apparently, is that the NSA must intercept at least some of these so-called "Wikimedia communications." But in an era when monthly

communications traffic on the Internet is measured in the tens if not hundreds of trillions, Wikimedia's alleged "extraordinarily high volume of internet communications" is merely a drop in the torrent of communications carried on the Internet and does not plausibly establish a likelihood that Wikimedia's "communications related to its users" are intercepted, much less retained and reviewed, during the course of Upstream surveillance. 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.

For these reasons, discussed more fully below, Plaintiffs have not plausibly alleged facts establishing, with the 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 Complaint must 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. 95-604, 95th Cong., 1st Sess., at 7 (1977). The statute was a response to revelations of unlawful Government surveillance directed at specific American citizens and political organizations. *Id*. at 7–8. FISA was intended to provide a check against such abuses by placing certain types of foreign-intelligence surveillance under the oversight of the FISC.[1]

[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).

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. 95-701, 95th Cong., 2d Sess., at 7, 34–35, 71 (1978) (the Act "does not deal with international signals intelligence activities" engaged in by the NSA or "electronic surveillance conducted" overseas); H.R. Rep. No. 95-1283(I), 95th Cong., 2d Sess., at 50–51 (1978).[4]

[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).

[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.

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. 110-209, 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 (May 1, 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. 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, therefore, as wire communications under FISA. 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.[5]

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. 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 that makes geography an increasingly irrelevant factor. Today, a single communication can transit the world even if the two people communicating are only located a

[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).

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 addressed this problem initially through the Protect America Act ("PAA"), Pub. L. No. 110-55 (2007),[6] and ultimately its successor statute, 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

[6] The PAA was enacted in 2007 to bring FISA "up to date with the changes in communications technology," while at the same time preserving "the privacy interests of persons in the United States" and addressing "degraded capabilities in the face of a heightened terrorist threat environment" that resulted from FISA's "requirement of a court order to collect foreign intelligence about foreign targets located overseas." S. Rep. No. 110-209, at 5–6 (2007). The PAA fulfilled these purposes by allowing the Government to conduct warrantless foreign-intelligence surveillance on targets, including U.S. persons, reasonably believed to be located outside the United States. *In re Directives*, 551 F.3d 1004, 1006 (F.I.S.C. Ct. Rev. 2008).

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 any acquisition conducted under the certification 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). Furthermore, the Government's exercise of its authority under Section 702

and its compliance with applicable statutory requirements is 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* Complaint for Declaratory and Injunctive Relief (ECF No. 1) (the "Complaint," or "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 accounts, addresses, or 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 the

selectors identified for tasking, and the providers furnish the NSA with electronic communications to or from these selectors. *See id.* (Plaintiffs do not challenge the legality of PRISM collection in this case. *See* 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 "backbone" networks, whereupon the providers must assist the Government in acquiring communications to, from, or otherwise containing these selectors while they cross 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.

Among other contributions to national security, Upstream collection has been critical to the Government's efforts to combat international terrorism and other threats to the United States and its interests abroad. Upstream is a "unique[ly] valu[able]" component of an intelligence program that "is critically important to maintaining our national security." PCLOB Report at 124; H.R. Rep. No. 112-645(II), 112th Cong., 2d Sess., at 3, 5 (2012); S. Rep. No. 112-174, 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 the disruption "of previously unknown terrorist plots," and is also used to "counter[ ] the efforts of proliferators 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," including "journalists, clients, experts, attorneys, civil society organizations, foreign government officials, and victims of human rights abuses." Compl. ¶¶ 2, 69, 78, 85, 90, 95, 100, 105, 110, 115.[7] Plaintiff Wikimedia Foundation ("Wikimedia") alleges that it also "engages in hundreds of billions of international communications each year" with "hundreds of millions of individuals"—whom it refers to as its "users"—who allegedly made over 16 billion visits to its web pages each month in 2014. *Id.* ¶¶ 2, 59, 64. Plaintiffs maintain that "[t]he ability to exchange information in confidence, free from warrantless government monitoring, is essential to each of [their] work," and that Upstream collection "violates [their] privacy and undermines their ability to carry out activities crucial to their missions." *Id.* ¶ 2. Plaintiffs sue on behalf of themselves and (with the exception of plaintiff National Association of Criminal Defense Lawyers ("NACDL")) purportedly their staffs. *Id.* ¶¶ 6–14. Wikimedia also purports to sue on behalf of its users, *id.* ¶ 6; the NACDL its members, *id.* ¶ 7; and the Nation Magazine its contributing journalists, *id.* ¶ 12.

According to Plaintiffs, "Upstream surveillance is intended to enable the comprehensive monitoring of international internet traffic," allowing the NSA to "cop[y] and review[ ] all international emails and other 'text-based' communications." *Id.* ¶ 42. 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

[7] Six of the plaintiffs in this case, 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).

internet data"; (3) content review, NSA "review[ ] [of] the copied communications—including their full content—for instances of its search terms [selectors]"; and (4) retention and use, the 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.* ¶ 43.

Based on the allegation that Upstream involves "intercepting, copying, and reviewing substantially all international text-based communications . . . as they transit telecommunications networks inside the United States," Plaintiffs assert that their communications "are intercepted, copied, and reviewed in the course of Upstream surveillance" as well. Compl. ¶¶ 49, 70, 79, 86, 91, 96, 101, 106, 111, 116. *See also id.* ¶¶ 1, 40, 42, 44 ("the NSA is seizing Americans' communications en masse" and "searching the contents of substantially all international text-based communications"); ¶¶ 38, 44 (the Government "intercept[s], cop[ies], and review[s] essentially everyone's internet communications").

Wikimedia also alleges that the Government intercepts, copies, and reviews a second category of "Wikimedia communications," specifically, "communications related to the activities of its users, who read and edit Wikimedia's projects and webpages and who use them to interact with each other." Compl. ¶ 62. According to the Complaint, Wikimedia "operates twelve free-knowledge projects" on the Internet, that is, websites such as Wikipedia and Wikibooks, and "provides the full contents of those projects to individuals around the world free of charge." *Id.* ¶¶ 6, 58–60. The content of these websites "is collaboratively researched and written by millions of volunteers," while Wikimedia "provides the technical infrastructure." *Id.* ¶¶ 59, 61. As described in the Complaint, Wikimedia users "view, edit, or contribute to" the content of its websites by sending "requests" across the Internet from their digital devices (such as personal computers or smartphones) to Wikimedia's servers, which upon receiving these requests transmit

the content of the requested web pages back to the users' devices. *Id.* ¶ 64. Wikimedia asserts that, as the operator of these websites, including Wikipedia, it "engages in an extraordinarily high volume of [such] communications," on average 16 billion user "visits" to its pages each month in 2014, numbering in the "hundreds of billions of international communications each year." *Id.* ¶¶ 59, 63, 64.

Plaintiffs maintain that the alleged interception, copying and 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." Compl. ¶¶ 70, 79, 86, 91, 96, 101, 106, 111, 116.

In addition to the claimed interception, copying, and review of their communications, Plaintiffs also allege that there is a "substantial likelihood" that their intercepted communications are "retained, read and disseminated" by the NSA. *Id.* ¶ 51. The retention, review, 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.* ¶¶ 53–54; *see also id.* ¶¶ 71, 72, 80, 87, 92, 97, 102, 107, 112, 117. Plaintiffs contend that 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.* ¶ 52.

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]." Compl. ¶¶ 2, 55, 56; *see also id.* ¶¶ 74, 75, 83, 88, 93, 98, 103, 108, 113, 118. 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.* ¶¶ 119–122. 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 all their communications acquired through Upstream surveillance. *Id.* ¶ 3; *id.* at 37 (prayer for relief).

ARGUMENT

I. LEGAL STANDARDS

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

The Complaint must be dismissed for lack of subject-matter jurisdiction, because it contains no well-pleaded allegations that plausibly establish Plaintiffs' standing. Under the pleading standard announced in *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007), and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), a complaint must contain "sufficient factual matter, accepted as true, to 'state a claim that is plausible on its face.'" *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 570); *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); *Sherrill v. Mayor & City Council of Baltimore*, 31 F. Supp. 3d 750, 764 (D. Md. 2014). 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). "No principle is more fundamental to the judiciary's proper role in our system of government," *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 341 (2006) (internal citation and quotation marks omitted), as "the case or controversy requirement defines with respect to the Judicial Branch the idea of the separation of powers on which the Federal Government is founded." *Allen v. Wright*, 468 U.S. 737, 750 (1984).

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); *Miller v. Montgomery Cnty., Md.*, 458 F. App'x 304, 308 (4th Cir. 2011). 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. Dept. of State Police*, 713 F.3d 745, 753 (4th Cir. 2013) (internal quotation marks and citation omitted). 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). If Plaintiffs cannot carry their threshold jurisdictional burden of adequately pleading their standing to sue, then "they may not litigate as suitors in the [C]ourts of the United States," *Valley Forge*, 454 U.S. at 475–76, and the Court must dismiss the case. *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 94 (1998).

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.") (internal quotation marks and 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, reviewed and disseminated" by the NSA. Compl. ¶¶ 49–52. 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, for which the 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 Review of Substantially All International Online Communications Transiting the United States.

Plaintiffs' allegations that they are injured through NSA interception, copying, and review of their online communications to identify communications containing NSA-targeted selectors are insufficient to establish the requisite Article III injury. This is so because they have not plausibly alleged that any of their online communications (or those of their "staffs," "users," or "members," as the case may be) are intercepted, copied, or reviewed at all during the Upstream collection process. As discussed *supra*, at 12, Plaintiffs allege that Upstream collection involves the initial interception and copying of online communications so they may be reviewed for selectors (such as e-mail addresses) associated with the targets of NSA surveillance; communications found to contain such selectors are retained in Government databases for further analysis and extraction of foreign-intelligence information. Compl. ¶¶ 42–

43. The assertion that *their* communications are intercepted, copied and reviewed in this manner is in turn predicated on the equally "bald allegation[ ]," *Iqbal*, 556 U.S. at 681, that the Government intercepts, copies, and reviews substantially all international [online] communications . . . as they transit telecommunications networks inside the United States." Compl. ¶¶ 1, 38, 40, 42, 44, 49, 70, 79, 86, 91, 96, 101, 106, 111, 116.

But these "bare assertions" are unaccompanied by "factual matter" that raises them "above the speculative level," and as such they are 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 facts that the Government has not publicly revealed. Thus, Plaintiffs can only speculate whether the NSA has ever intercepted, collected, or reviewed communications of theirs in connection with the Upstream process. *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 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." Compl. ¶ 37. But a nebulous allegation that "FAA surveillance" is "wide-ranging" "stops short"—far short—of plausibly establishing that Upstream surveillance involves the interception, copying, and review of all or even "substantially all," Compl. ¶¶ 1, 42; *Twombly*, 550 U.S. at 556–57, international

online communication carried on U.S. telecommunications networks. 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; Compl. ¶¶ 39–40.

The public documents alluded to by Plaintiffs fall short in the same ways. Plaintiffs first refer to a report by the Office of the Director of National Intelligence ("ODNI") stating that, "in 2013, the [G]overnment relied on the FAA to target 89,138 individuals, groups, or organizations for surveillance." Compl. ¶ 37; *see* ODNI, Statistical Transparency Report Regarding Use of National Security Authorities (June 26, 2014) ("ODNI Transparency Report") (Exh. 3, hereto).[8] Specifically, the ODNI Transparency Report revealed that in 2013 the Intelligence Community relied on Section 702 to conduct surveillance of an estimated 89,138 targets (*i.e.*, particular persons, groups, or organizations at whom intelligence collection is directed). ODNI Transparency Report at 2. This figure lends no support to Plaintiffs' allegation that the NSA intercepts all international online communications traversing the United States. First, the ODNI transparency report does not reveal how many of the 89,138 persons, groups, and organizations targeted for surveillance under Section 702 were targeted for Upstream as opposed to PRISM surveillance. ODNI Transparency Report at 2. And even if all 89,138 were targets of Upstream surveillance (out of approximately three billion individuals and organizations that communicate via the Internet, *see* Declaration of Robert T. Lee (Exh. 4, hereto)[9] ("Lee Decl."), ¶ 14,[10] that

[8] 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).

[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] 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 computer forensics,

says nothing about the scale on which Upstream collection is conducted in order to maintain surveillance on those targets. Much less does it succeed in raising the allegation that the NSA intercepts, copies, and reviews all international online communications sent or received in the United States "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. Compl. ¶ 37; [*Caption Redacted*], 2011 WL 10945618, at *9 (F.I.S.C. Oct. 3, 2011) ("Oct. 3, 2011 FISC Op.").[11] 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., ¶¶ 13–19. Nothing in the FISC's October 3, 2011 opinion suggests that the NSA, in order to collect this tiny percentage of

---

vulnerability, and exploit discovery, intrusion detection/prevention, and incident response," Mr. Lee is "currently the curriculum lead and author for digital forensic and incident response training at the SANS Institute." *Id.* Previously, Mr. Lee served in the U.S. Air Force, where, in addition to serving in a military operational unit focused on information warfare, he "led a team conducting computer crime investigations, incident response, and computer forensics." *Id.* He has since worked with law enforcement and various members of the intelligence community "as a technical lead" for teams engaged in, among other projects, "computer forensic and security software development" and "cyber-forensics." *Id.* Mr. Lee has also co-authored a book in this field entitled, *Know Your Enemy*, 2nd Edition.

[11] In that decision the FISC largely approved the NSA's targeting and minimization procedures as consistent with statutory and constitutional requirements, but concluded that the targeting and minimization procedures did not meet statutory or constitutional requirements 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 that 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).

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

Lastly, Plaintiffs rely on the PCLOB and PRG Reports, Compl. ¶ 37, but these reports simply repeat the figures contained 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 "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. Wikimedia Cannot Establish Its Standing by Alleging that It Engages in Such an "Extraordinarily High Volume" of International Internet Communications that Those Communications Must Be Intercepted, Copied, or Reviewed in the Upstream Collection Process.

Alone among the Plaintiffs, Wikimedia Foundation ("Wikimedia") alleges that it "engages in an extraordinarily high volume of internet communications," which it describes as communications "related to the activities of its users," Compl. ¶¶ 62, 63, and alleges that these communications "are intercepted, copied, and reviewed in the course of Upstream surveillance." *Id.* ¶ 70. Wikimedia explains that these "communications related to the activities of its users" are of two types. *Id.* ¶ 62. The first involves a "user . . . view[ing], edit[ing], or contribut[ing] to a Wikimedia Project webpage," *id.* ¶ 64, communications that allegedly occurred over 16 billion times each month in 2014, *id.* ¶ 59. The second involves users "interact[ing] more directly" with one another by sending email on Wikimedia accounts or by "interact[ing] in small or limited

groups" on restricted Wikimedia websites. *Id.* ¶ 65. According to Wikimedia, it "engages in hundreds of billions of [these] international communications each year." *Id.* ¶ 64.

Wikimedia does not expressly say so in the Complaint, but it appears to advance a theory of standing that the above "communications related to the activities of its users" are so numerous that in all likelihood the NSA, regardless of Upstream's scope or focus, *must* intercept, copy, and review at least some of those communications. As a matter of fact, however, the number of these "communications related to [Wikimedia's] users," Compl. ¶ 66, represents an relatively small portion of total Internet traffic, and does not support the inference that the NSA likely intercepts Wikimedia's communications. And, as a matter of law, Wikimedia's theory of standing is foreclosed by the Supreme Court's decision in *Amnesty International*.

1. Wikimedia's Communications Related to the Activities of Its Users Represent Only a Small Proportion of the Total Volume of Communications Carried on the Internet.

The "hundreds of billions of international communications" in which Wikimedia claims it engages in each year, Compl. ¶ 64, is in fact an relatively small portion of global Internet traffic. Traffic on the Internet includes "email, web browsing, social media, audio and video streaming, Voice Over Internet Protocol (Internet telephony), video conferencing, and peer to peer sharing." Lee Decl. ¶ 15. In terms of units of information, this traffic totals about 2.2 billion gigabytes of data traversing the Internet per day, or about 800 billion gigabytes per year. *Id.* Wikimedia does not plead what portion of that Internet traffic may be attributed to its communications.

Instead, Wikimedia principally describes the volume of its communications in terms of the alleged "hundreds of billions" of "communications related to the activities of its users" occurring each year. Compl. ¶¶ 62–64. Wikimedia treats as a communication each occasion on which a user "view[s], edit[s], or contribute[s] to a Wikimedia . . . webpage." Compl. ¶ 64.

Wikimedia alleges that "users visited Wikimedia 'pages' or entries over 16 billion times each month during 2014," *id.* ¶ 59, or about 192 billion times per year. That number pales in comparison, however, to the total number of emails sent, to take just one example of a text-based Internet communication. There are about 183 to 202 billion emails sent *every day*, *see* Lee Decl. ¶ 16, which means approximately 5.49 to 6 *trillion* emails are sent each month. Thus, the alleged 16 billion webpage views per month to Wikimedia's web pages correspond to about three-tenths of one percent (0.3%) of just the e-mail traffic carried on the Internet. *See id.* ¶ 15. That percentage becomes even smaller when other traffic carried on the Internet is also taken into consideration. For example, there are approximately 750 million tweets each day, *id.* ¶ 19 n.17, or about 28 trillion per year. The annual number of Wikimedia web page views corresponds to about one-quarter of one percent (0.25%) of the combined traffic attributable to just these two text-based forms—tweets and email—of Internet communications.

Wikimedia's 16 billion monthly (192 billion yearly) web page views must also be considered in light of the number of visits to other websites. As Mr. Lee observes in his declaration, "[c]ertain commercial organizations track website usage," one of which is known as "Similar Web." Lee Decl. ¶ 18. Similar Web estimates that Facebook.com has about 357 billion web page views per month, or about 4.3 trillion each year, and that Google.com has about 208 billion web page views per month, or about 2.5 trillion per year. *See id.* ¶ 19. In comparison, therefore, Wikimedia's web page views of 16 billion per month (192 billion per year) constitute only about 2.8% of the total web page views of these top two websites combined. And Wikimedia's portion would only fall when one takes into account that there are approximately 236 million other websites on the Internet that are active in some way. *See id.* ¶ 17.[12]

[12] For example, if one adds Youtube's web page views of 147 billion per month, *see* Lee Decl. ¶ 19, then Wikimedia's web page views are only about 2.25% of the webpage views of these top three web sites combined.

Nor does the number of Wikimedia's "editors" support an inference that its user-related communications have likely been intercepted, copied, or reviewed in the Upstream collection process. Wikimedia alleges that "[m]ore than 89 million registered and unregistered users have edited a Wikimedia page" and that "the majority" of these users "are located abroad." Compl. ¶ 63. This number includes, presumably, editors who contributed to Wikipedia at any time over the last fourteen years since the site was launched in 2001, *see* http://en.wikipedia.org/wiki/History_of_Wikipedia (last visited, May 24, 2015). Thus, Wikimedia's 89 million editors include those who made contributions in the seven years *before* Section 702 was enacted in 2008, *see* FISA Amendments Act of 2008, Pub. L. No. 110-261 (2008), many of whom may not have contributed to any Wikimedia websites since the challenged Upstream program began. Even assuming each of those 89 million editors made contributions after Upstream collection began, there are now "approximately 3.0 billion Internet users worldwide," Lee Decl. ¶ 14, meaning that Wikimedia's editors constitute only 2.9% of total global Internet users.[13] That percentage falls dramatically when the number of global Internet users is compared to the number of "active" Wikimedia editors for all projects (83,597), *see* https://reportcard.wmflabs.org/#core-graphs-tab (last visited, May 21, 2015), or the number of "very active" Wikimedia editors (12,597), *see* https://reportcard.wmflabs.org/#secondary-graphs-tab (last visited, May 21, 2015). The active editors make up only 0.0029% and the very active editors make up only 0.0004% of the total number of global Internet users.

In short, Wikimedia's "extraordinarily high volume of internet communications" is by all appearances miniscule when compared to the total volume of Internet communications traffic.

[13] Wikimedia is also asking the Court to presume that these 89 million registered and unregistered users are 89 million different people. That may not necessarily be correct. The use of multiple accounts by the same person (for numerous improper purposes) is of sufficient concern to Wiki Projects that it has its own name for the phenomenon, "sock puppetry." *See* http://en.wikipedia.org/wiki/Wikipedia:Sock_puppetry (last visited May 21, 2015).

The raw number of these "hundreds of billions" of communications each year does not itself establish that the NSA must intercept, copy, and review "Wikimedia communications related to the activities of its users" during the Upstream collection process.

2. Insofar as Wikimedia Suggests that the Volume of Its Communications Makes it Substantially Likely that Some of Them Have Been Intercepted, Copied, and Reviewed in the Upstream Collection Process, that is Legally Insufficient, Under *Amnesty International*, to Establish Standing.

Wikimedia's apparent theory of standing is not only factually unsubstantiated, it has been foreclosed as a matter of law by Supreme Court precedent. In *Amnesty International*, the plaintiffs challenged the legality of Section 702 of the FISA on the day it was enacted by Congress. *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, plaintiffs claimed instead that they had standing because there was an "objectively reasonable likelihood" that plaintiffs' 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 based its conclusion 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 was authorized and highly motivated, for counter-terrorism purposes, to intercept, and (2) that the record showed the Government had in fact intercepted such communications on thousands of occasions in the past. *Id.* at 1156–59.

Wikimedia tacitly advances a "likelihood" theory of standing that is remarkably similar to the one rejected in *Amnesty International*. Like the plaintiffs in that case, Wikimedia "fail[s] to offer" any well-pled allegations "that [its] communications have been monitored under" Upstream, *id.* at 1148, and instead relies on speculation that, given the volume of its international "communications," it is reasonably likely that Wikimedia's communications have been, or imminently will be, intercepted, copied, and reviewed during the Upstream collection process. This 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 Complaint must adequately plead facts plausibly demonstrating that so-called "Wikimedia communications related to the activities of its users" 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 had plausibly alleged a likelihood that the NSA intercepts, copies, or reviews "Wikimedia communications related to the activities of its users," Compl. ¶ 62, and even if that alleged likelihood were sufficient, under *Amnesty International*, to confer Article III standing, Plaintiff Wikimedia would still lack prudential standing to challenge the alleged interception, copying, and review of these "communications related to its users," *id.* ¶ 66. This is so because Wikimedia does not have third-party standing to raise the legal rights and interests of these unidentified Internet users.

As discussed above, by "communications related to its users" Wikimedia principally means users visiting its web pages, to read or sometimes edit their content, or to communicate with one another through a Wikimedia website. *Id.* ¶ 62. According to the Complaint, these communications involve electronic "requests" transmitted via the Internet from a user's electronic device (such as a desktop or laptop computer, or smartphone) to the Wikimedia server that hosts that web page. After receiving the user's request, the Wikimedia server transmits the requested content from the webpage back to the user's device. *Id.* ¶ 64.

That is a fair if incomplete description of the process by which typical Internet users view or download information displayed on Internet websites. 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.[14] 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.* ¶¶ 7–9.[15] 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.* ¶¶ 8–9. Upon receiving the request, the website's host computers automatically generate and send a return message that includes the information requested by the user 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.* ¶ 9.

[14] 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 "Internet café" such as a Starbucks. Lee Decl. ¶ 11a–e.

[15] The IP address may be a static (permanent) address, such 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 practices of the ISP. Lee Decl. ¶ 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.* ¶ 11.[16]

In short, what Plaintiff Wikimedia calls "Wikimedia communications related to the activities of its users," Compl. ¶ 62, are nothing more than automated transmissions of publicly available information displayed on Wikimedia 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.* ¶ 59; Wikimedia provides only the "technical infrastructure" needed to post it on the World Wide Web, *id.* ¶ 61.[17] 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.*

[16] 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. ¶ 11.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.* ¶ 11.b.

[17] As stated in the overview to Wikimedia's own Terms of Use for contributors, authors, and editors (available at http://wikimediafoundation.org/wiki/Terms_of_Use) (last visited on May 28, 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.").

¶¶ 6, 58.[18] 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 users, who designate the content they wish to receive. Lee Decl. ¶ 9. Nor, finally, does Wikimedia know (or care, *see* Compl. ¶ 58) to whom it sends the information. It knows only the IP addresses associated with the communications in which these requests are received. Lee Decl. ¶¶ 8–11. It knows nothing about the actual identities of the individuals who typically view or download contents from its websites on a daily basis unless those individuals specifically provide that information to the websites. *Id.* ¶¶ 10–12.[19]

It comes as little surprise, therefore, that the Complaint identifies no privacy interest *of Wikimedia's* in these "communications related to the activities of its users." Rather, it speaks only in terms of *users'* privacy interests. According to the Complaint, "Wikimedia's communications related to its users activities 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." Compl. ¶ 66; *see also id.* ¶ 68 (alleging that "Wikimedia possesses a large volume of sensitive information *about its users*" and "transmits a large volume of sensitive information *about those*

[18] *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).

[19] Wikimedia's Privacy Policy informs its users that "[w]e believe that you shouldn't have to provide personal information to participate in the free knowledge movement. You do not have to provide things like your real name, address, or date of birth to sign up for a standard account or contribute content to the Wikimedia sites." http://wikimediafoundation.org/wiki/Privacy_policy (last visited, May 26, 2015).

users every day") (emphasis added). Thus, even if Wikimedia adequately alleged NSA interception, copying and review of so-called "communications related to its users," the Complaint alleges no resulting injury except (arguably) to the privacy of its users. [20]

Wikimedia lacks standing, however, to assert the privacy rights of the unidentified users who happen to view, download, or 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 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 communications related to the activities of its users are concerned.

First, as discussed *supra*, at 31, the Complaint does not even purport to identify an injury to Wikimedia's privacy interests from the alleged NSA interception, copying, and review of transmissions from Wikimedia websites to its users. *See generally* Compl. ¶¶ 58–68. Second, the Complaint does not allege, and could not allege, a "close relationship" between Wikimedia and the anonymous "users" of its websites whose identities are entirely unknown to it. *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"). And even if Wikimedia met

[20] Wikimedia also alleges no privacy interest of its own in the communications through which its users "interact" with one another. The Complaint describes these communications as including e-mail among registered users of Wikimedia accounts, restricted-access wikis (collaborative web pages), and user mailing lists. Compl. ¶ 65. Although Wikimedia allegedly supplies the technical infrastructure to make these user-to-user communications possible, *see id.*¶ 61 (much like a typical Internet service provider), Wikimedia likewise identifies no privacy interest it possesses in these communications between and among users.

these first two requirements, Wikimedia has not alleged any hindrance to users' ability to protect their own interests by bringing their own suits challenging Upstream collection. That omission alone defeats Wikimedia's standing to assert their legal rights. *Freilich*, 313 F.3d at 215. In any event, Wikimedia could not plausibly allege any such hindrance, given the presence of eight other plaintiffs to this suit alone, and the multiple plaintiffs who have challenged Upstream collection in *Jewel v. NSA*, 2015 WL 545925, at *1–2 (N.D. Cal. Feb. 10, 2015).

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 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 have failed to plausibly allege initial NSA interception, copying, and 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 alleged an initial interception, copying, and review, Plaintiffs would still fail to establish their standing to challenge the alleged subsequent retention, review, 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' claim that the NSA likely retains their online communications because they correspond with likely targets of Upstream surveillance concerning topics that meet the

definition of foreign-intelligence information fails to establish Article III standing. Specifically, 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." Compl. ¶¶ 53–54; *see also id.* ¶¶ 71, 72, 80, 87, 92, 97, 102, 107, 112, 117. 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. 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." Compl. ¶ 51.

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. 5, 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." Compl. ¶ 51 (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 (internal citation and quotation marks 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.[21]

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 as to whether any asserted acquisition occurred in connection with Upstream collection as opposed to PRISM, some other statutory authority under FISA, or Executive Order 12333, they cannot satisfy the

[21] Indeed, Plaintiffs' allegations here often contain less specificity than the declarations the Court found wanting in *Amnesty International*. *Compare* Compl. ¶¶ 84–88 (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. in *Amnesty International* ¶¶ 4–9 (attached as Exh. 6, 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).

requirement of demonstrating 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, which allege that the NSA retains, reads, and disseminates their own communications, Plaintiff NACDL alone alleges the retention, review and dissemination of its individual members' communications, and purports to sue on their behalf. Compl. ¶¶ 7, 80-81.[22] Specifically, 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.* ¶ 80. 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.* ¶ 81. As discussed in Section III.A above, *see supra*, at 31-33, such "necessarily conjectural" assertions are insufficient for purposes of establishing standing. *Amnesty Int'l*, 133 S. Ct. at 1149. But in addition to this shortcoming in NACDL's allegations regarding its own standing, NACDL also fails to establish its associational standing to sue on its members' behalf.

An organization such as NACDL "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 (quoting *Md. Highways Contractors Ass'n v.*

[22] Plaintiffs Amnesty International USA and PEN American Center also state in passing that they sue on behalf of their members, *see* Compl. ¶¶ 9, 10, but they fail to advance any allegations of injury to their members separate and apart from their alleged organizational harms. *See* Compl. ¶¶ 89–98. Accordingly, NACDL alone purports to bring claims on behalf of its members.

Maryland, 933 F.2d 1246, 1250 (4th Cir. 1991) (citing *Hunt v. Washington State Apple Advertising Comm'n*, 432 U.S. 333, 343 (1977))).

In connection with 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* had suffered or would suffer harm.'" *Id.* at 184 (quoting *Summers v. Earth Island Inst.*, 555 U.S. 488, 498 (2009) (emphasis supplied by the Court of Appeals)); *see also United Food & Commercial Workers v. Brown Group, Inc.*, 517 U.S. 544, 555 (1996) ("an organization suing as representative" must "include at least one member with standing to present, in his or her own right, the claim (or the type of claim) pleaded by the association")).[23] This aspect of the test is grounded in "the constitutional requirement of a case or controversy," *United Food & Commercial Workers*, 517 U.S. at 554–55 (quoting *Warth*, 422 U.S. at 511), and is therefore "an Article III necessity for an association's representative suit," *id.* at 555. *See also Summers*, 555 U.S. at 492–93.

In accordance with that requirement, the Supreme Court has specifically rejected a theory of representational standing based on "a statistical probability that some of [an organization's] members are threatened with concrete injury." *Summers*, 555 U.S. at 497. In particular, the Court held that an uncontested showing by the plaintiffs in that case that "it [was] possible—perhaps even likely—that one individual [would] meet all of [the] criteria" for standing "[did] not suffice." *Id.* at 499. The Court was unequivocal: such an "approach to the law of organizational standing would make a mockery of [its] prior cases." *Id.* at 498.

[23] *See also, e.g.*, *Natural Resources Def. Council v. Watkins*, 954 F.2d 974, 978 n.6 (4th Cir. 1992); *Ohio Valley Envt'l Coal. v. United States Army Corps of Eng'rs*, 2014 WL 4102478, at *10 (S.D. W. Va. Aug. 18, 2014) ("The plaintiffs' standing . . . must lie in the standing of the one member that they specifically allege to be affected . . . . the court finds that Sierra Club and WVHC do not have standing, as they have not put forth any member of their organization that has alleged a concrete injury.").

Yet that is the very approach NACDL urges here. Rather than identifying any member whose communications NSA has allegedly retained as part of the Upstream collection process, NACDL alleges only "*a substantial likelihood* that the NSA retains, reads, and disseminates international communications of NACDL's members," Compl. ¶ at 80 (emphasis added), and refers to a group of members that it claims "*is especially likely* to have [its] communications retained, read, and disseminated in the course of Upstream surveillance," *id.* ¶ 81 (emphasis added). 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 one member will meet the criteria for standing, "that speculation does not suffice," 555 U.S. at 499; "[i]n part because of the difficulty of verifying the facts upon which such probabilistic standing depends," an organization must identify specific members "who have suffered the requisite harm." *Id.* Because NACDL has not done so, *see generally id.* ¶¶ 77–83, it has failed to establish representational standing and its claims on behalf of its members should be dismissed.

* * *

In sum, the Complaint fails to establish that any of the Plaintiffs, or any member of NACDL, has sustained an injury that is "fairly traceable to" retention, review, and dissemination of online communications in connection with Upstream surveillance. *Amnesty Int'l*, 133 S. Ct. at 1150. Under *Amnesty International*, therefore, even if Plaintiffs had demonstrated their standing to challenge an alleged initial interception, copying, and review of their communications, they would still lack standing to contest the subsequent alleged retention, review and dissemination.

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

Plaintiffs' claim that Upstream collection inhibits their ability to conduct their work is also an inadequate basis under *Amnesty International* to establish standing. The 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 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* Compl. ¶ 55. As a result, Plaintiffs 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.* ¶ 56; *see also id.* ¶¶ 74, 75, 83, 88, 93, 98, 103, 108, 113, 118.

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' claims regarding Upstream collection. Plaintiffs' 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 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."[24] Compl. ¶ 56; *see also id.* ¶¶ 74, 75, 83, 88, 93, 98, 103, 108, 113, 118. 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

[24] In various sections of the Complaint, Plaintiffs tailor these allegations to the individual circumstances of each plaintiff. At their core, however, all Plaintiffs allege the same speculative grievances surrounding the alleged harm to their ability to conduct their work.

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 "chill" upon the willingness of third parties to communicate with Plaintiffs "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 Complaint contains no factual support for Plaintiffs' 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: May 29, 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/ Rodney Patton
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 7320
Washington, D.C. 20044
Phone: (202) 305-7919
Fax: (202) 616-8470
Rodney.patton@usdoj.gov

Counsel for Defendants