No. 15-2560

IN THE UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

WIKIMEDIA FOUNDATION, *et al.*,

Plaintiffs-Appellants,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants-Appellees.

On Appeal from the United States District Court
for the District of Maryland at Baltimore

BRIEF FOR DEFENDANTS-APPELLEES

BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General

ROD J. ROSENSTEIN
United States Attorney

DOUGLAS N. LETTER
H. THOMAS BYRON III
CATHERINE H. DORSEY
MICHAEL SHIH
Attorneys, Appellate Staff
Civil Division, Room 7236
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530
(202) 514-3469

TABLE OF CONTENTS

Page

INTRODUCTION 1

STATEMENT OF JURISDICTION 3

STATEMENT OF THE ISSUE 3

PERTINENT STATUTES AND REGULATIONS 3

STATEMENT OF THE CASE 4

A. Statutory Background: The Foreign Intelligence Surveillance Act and the 2008 Amendments 4

B. Factual Background: Upstream Collection Under Section 702 8

C. Proceedings Below 11

1. Plaintiffs' Complaint 11

2. The Government's Motion to Dismiss 14

a. Lee Declaration 16

b. Salzberg Declaration 18

3. The District Court's Decision 20

SUMMARY OF ARGUMENT 22

STANDARD OF REVIEW 25

ARGUMENT 25

I. PLAINTIFFS FAIL TO ALLEGE THAT THE UPSTREAM PROGRAM IS LIKELY TO INTERCEPT THEIR COMMUNICATIONS. 25

A. Plaintiffs Do Not Allege A "Certainly Impending" Injury Based On Interception, Copying, And Selector Review Of Their Internet Communications. 28

1. Plaintiffs Cannot Rely On Their Speculative Claim That The NSA Is Intercepting "Substantially All" International Text-Based Communications. 29

2. Wikimedia Has Not Plausibly Alleged That Its Communications Will Be Intercepted. 37

3. Defendants' Declarations Further Support The District Court's Dismissal Of The Complaint. 43

4. Even If Some Of Their Communications Were Likely To Be Intercepted, Plaintiffs Failed To Allege A Cognizable Injury. 45

B. Plaintiffs Have Not Alleged That Retention And Potential Analysis Of Their Communications Is A "Certainly Impending" Injury. 48

II. Plaintiffs' Arguments As To Why *Amnesty International* Is Inapplicable Are Wrong. 51

III. The District Court Properly Rejected Plaintiffs' Other Asserted Bases for Standing. 53

A. *Amnesty International* Forecloses Plaintiffs' Argument That They Have Been Compelled to Take Measures To Avoid Surveillance. 53

B. Plaintiffs Have Not Plausibly Alleged A First Amendment Violation. 56

C. Wikimedia Had Not Plausibly Alleged Standing On Behalf Of Any Third Party. 56

CONCLUSION 57

CERTIFICATE OF COMPLIANCE

CERTIFICATE OF SERVICE

ADDENDUM

TABLE OF AUTHORITIES

Cases: **Page(s)**

Adams v. *Bain*,
697 F.2d 1213 (4th Cir. 1982) 43

Ashcfroft v. *Iqbal,*
556 U.S. 662 (2009) 20, 25, 26

Bell Atlantic Corp. v. *Twombly*,
550 U.S. 544 (2007) 25

Clapper v. *Amnesty International, USA*,
133 S. Ct. 1138 (2013) 2, 15, 22, 26, 27, 28, 30, 31, 32, 35, 42, 49, 50, 53, 54, 55, 56, 57

David v. *Alphin*,
704 F.3d 327 (4th Cir. 2013) 26

Doe v. *Virginia Dep't of State Police*,
713 F.3d 745 (4th Cir. 2013) 56

Freilich v. *Upper Chesapeake Health, Inc.*,
313 F.3d 205 (4th Cir. 2002) 57

Kowalski v. *Tesmer*,
543 U.S. 125 (2004) 56

Laird v. *Tatum*,
408 U.S. 1 (1972) 56

Lane v. *Holder*,
703 F.3d 668 (4th Cir. 2012) 25

Obama v. *Klayman*,
800 F.3d 559 (D.C. Cir. 2015) 32, 42

SD3, LLC v. *Black & Decker (U.S.) Inc.*,
801 F.3d 412 (4th Cir. 2015) 32, 33

United States ex rel. Vuyyuru v. *Jadhav*,
555 F.3d 337, 347-48 (4th Cir. 2009) 16

Valley Forge Christian Coll. v. *Americans United for Separation of Church & State*,
454 U.S. 464 (1982) 56

Velasco v. *Gov't of Indonesia*,
370 F.3d 392, 398 (4th Cir. 2004) 16

Statutes:

Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.* 4
50 U.S.C. § 1801(e) 4
50 U.S.C. § 1801(f) 5
50 U.S.C. § 1801(f)(2) 6
50 U.S.C. § 1801(m) 40
50 U.S.C. § 1803(a) 4
50 U.S.C. § 1804(a) 4
50 U.S.C. § 1805 4
50 U.S.C. § 1805(a)(2) 4
50 U.S.C. § 1803(a) 4
50 U.S.C. § 1881(a) 7, 40
50 U.S.C. § 1881(b) 7
50 U.S.C. § 1881(g) 7

FISA Amendments Act of 2008,
Pub. L. No. 110-261, 122 Stat. 2436 6
50 U.S.C. § 1881a 7, 31
50 U.S.C. § 1881a-1881g 6, 31
50 U.S.C. § 1881a(a) 7, 8
50 U.S.C. § 1881a(b) 7, 8, 40
50 U.S.C. § 1881a(c)(1) 7
50 U.S.C. § 1881a(d) 8
50 U.S.C. § 1881a(g) 7
50 U.S.C. § 1881a(g)(1) 7
50 U.S.C. § 1881a(g)(2) 7
50 U.S.C. § 1881a(h) 10
50 U.S.C. § 1881a(i) 8

28 U.S.C. § 1291 3

28 U.S.C. § 1331 3

42 U.S.C. § 2000ee.....9

Legislative Materials:

H.R. Rep. 112-645 (2012).....6

Modernization of the Foreign Intelligence Surveillance Act: Hearing Before the S. Select Comm. on Intelligence, 110th Cong. (May 1, 2007) 5, 6

S. Rep. No. 95-604 (1977).....4

S. Rep. No. 95-701 (1978).....5

S. Rep. No. 112-174 (2012).....11

Other Authorities:

Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies (Dec. 12, 2013)..... 9, 11

Office of the Dir. of Nat'l Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities* (Apr. 22, 2015) 35, 36

Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the FISA* (July 2, 2014).....8, 9, 10, 11, 36, 48, 49, 54, 55

INTRODUCTION

Plaintiffs, nine organizations, seek to contest the legality of "Upstream" surveillance, a program under which the National Security Agency (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 such individuals by acquiring online communications to, from, or "about" those targets as they transit certain Internet "backbone" networks of U.S. telecommunications service providers. Upstream surveillance is conducted under the authority of Section 702 of the Foreign Intelligence Surveillance Act (FISA), pursuant to targeting and minimization procedures that have been approved by the Foreign Intelligence Surveillance Court 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.

The sole issue on appeal is whether the district court correctly held that plaintiffs lack Article III standing because they failed to allege a cognizable injury. Plaintiffs focus on two theories of standing; neither, however, is supported by sufficient factual allegations to plausibly state a claim of concrete, imminent injury. First, plaintiffs allege that, in order to reliably identify communications authorized for collection, Upstream surveillance "must" intercept, copy, filter, and review

"substantially all" international online communications—including theirs—transiting U.S. telecommunications networks. In the alternative, plaintiffs assert that, because plaintiff Wikimedia engages in over a trillion online communications each year, it is "virtually certain" that the NSA will intercept at least one of its communications. As the district court ruled, neither theory confers standing on plaintiffs, collectively, or on Wikimedia, individually, because both theories rest on speculation about the scope and scale of Upstream surveillance—details that remain classified.

The Supreme Court's recent decision in *Clapper* v. *Amnesty International, USA*, 133 S. Ct. 1138 (2013), confirms that plaintiffs' allegations are insufficient to confer standing. In that case, the Supreme Court held that a similar set of organizations—six of which are also plaintiffs here—lacked standing to challenge the constitutionality of FISA Section 702 because it was "speculative" whether "the Government [would] target the communications of non-U.S. persons with whom [those organizations] communicate," whether the Government would succeed in intercepting those communications, and whether those organizations would "be parties to the particular communications that the Government intercepts." *Id.* at 1148-50.

Plaintiffs' theories of standing in this case rest on a similarly "speculative chain of possibilities," *Amnesty Int'l*, 133 S. Ct. at 1150, and therefore fail to state a plausible claim that, under Upstream surveillance, some of their international online communications are being intercepted, copied, and reviewed to determine whether they are to, from, or "about" NSA's surveillance targets. In any event, plaintiffs have

failed to plausibly allege how temporary interception and non-human review of their communications, solely to determine whether they are to, from, or "about" foreign surveillance targets, could infringe their cognizable privacy interests.

STATEMENT OF JURISDICTION

Plaintiffs invoked the district court's jurisdiction under 28 U.S.C. § 1331. JA 31. On October 23, 2015, the district court granted the government's motion to dismiss for lack of jurisdiction and entered final judgment for the government. JA 204. Plaintiffs filed a notice of appeal on December 15, 2015. JA 205. This Court has jurisdiction under 28 U.S.C. § 1291.

STATEMENT OF THE ISSUE

Whether the district court properly dismissed plaintiffs' complaint for lack of standing because no court could draw a reasonable inference, based solely on plaintiffs' speculation about the scope and scale of Upstream surveillance, that the injuries plaintiffs allege—(1) interception, copying, filtering, and reviewing for targeted selectors their international text-based communications, and (2) retention and potential analysis of communications authorized for collection—are "certainly impending."

PERTINENT STATUTES AND REGULATIONS

Pertinent statutes are reproduced in the addendum to this brief.

STATEMENT OF THE CASE

A. Statutory Background: The Foreign Intelligence Surveillance Act and the 2008 Amendments

The Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1801 *et seq.*, "regulate[s] the use of electronic surveillance within the United States for foreign intelligence purposes." S. Rep. No. 95-604, at 7 (1977). FISA was enacted in the aftermath of Watergate, which revealed incidences of unlawful electronic surveillance directed at specific United States citizens and political organizations. *Id.* at 7-8. FISA provides a check against such activities by placing certain types of electronic surveillance under the oversight of the Foreign Intelligence Surveillance Court (FISC), an Article III court whose eleven members are selected by the Chief Justice of the United States from the ranks of the federal judiciary. *See* 50 U.S.C. § 1803(a).

Generally, before the government may conduct "electronic surveillance," as defined in FISA, to obtain foreign intelligence information, it must first obtain authorization from the FISC. 50 U.S.C. §§ 1803(a), 1804(a), 1805; *see also id.* § 1801(e) (defining "foreign intelligence information"). When enacted, FISA required the government to demonstrate probable cause to believe that the target of its surveillance "is a foreign power or an agent of a foreign power," and that the facility or place at which 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).

FISA originally applied only to "electronic surveillance" of communications to or from (or other information about) persons located in the United States. 50 U.S.C. § 1801(f). Congress intentionally excluded from FISA's reach the vast majority of government surveillance then conducted abroad—including surveillance targeted at U.S. citizens living abroad or surveillance that resulted in the incidental acquisition of communications to or from U.S. persons or individuals in the United States. S. Rep. No. 95-701, at 34-35, 71 (1978) (explaining that FISA "does not deal with international signals intelligence activities" or "electronic surveillance conducted" overseas).

By 2007, Congress recognized that FISA's definition of "electronic surveillance" had become obsolete because it was "tie[d] . . . to a snapshot of outdated technology." *Modernization of the Foreign Intelligence Surveillance Act: Hearing Before the S. Select Comm. on Intelligence*, 110th Cong. 19 (May 1, 2007) (FISA Hearing). 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 therefore potentially qualified as wire communications subject to FISA when intercepted in the United States. Thus, many forms of electronic surveillance that fell outside FISA's reach when enacted were now potentially subject to its provisions due to changes in technology. *Id.* 18-19.

Moreover, 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. FISA Hearing 19; 50 U.S.C. § 1801(f)(2). Technological advances rendered this distinction outmoded, too, because today's integrated communications grid makes it possible for an electronic communication to "transit the world even if the two people communicating are only located a few miles apart." FISA Hearing 19.

This evolution of communications technology forced the government to expend significant time and resources seeking FISC approval for electronic surveillance that Congress had originally placed outside FISA's scope. FISA Hearing 19. Moreover, those delays led to the loss of vital foreign intelligence. H.R. Rep. 112-645, pt. 1, at 2 (2012) ("[T]he Intelligence Community was not collecting approximately two-thirds of the foreign intelligence information that it [had previously] collected[.]"). To rectify the situation, Congress devised a "technology-neutral" framework to govern electronic surveillance of foreign targets, one that focuses 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 Hearing 46.

The resulting FISA Amendments Act of 2008 (FAA), Pub. L. No. 110-261, 122 Stat. 2436 (2008), created new procedures permitting the executive branch to acquire foreign-intelligence information by targeting non-U.S. persons located abroad. *See* 50 U.S.C. §§ 1881a-1881g.

The new FISA Section 702, codified at 50 U.S.C. § 1881a, sets forth the process for obtaining authorization for "targeting of [non-U.S.] persons reasonably believed to be located outside the United States to acquire foreign intelligence information." *Id.* § 1881a(a), (b), (g). Generally, the Attorney General and the Director of National Intelligence initiate the process by submitting a "certification" to the FISC. *Id.* § 1881a(g)(1). Among other things, that certification must attest that a significant purpose of the acquisition is to obtain foreign-intelligence information from or with the help of an electronic communication service provider, and that the acquisition will be conducted in accordance with targeting and minimization procedures that satisfy requirements set forth in the statute. *Id.* § 1881a(g)(2). In addition, acquisitions may only be conducted in accordance with appropriately adopted and approved targeting and minimization procedures. *Id.* § 1881a(c)(1). The FISC reviews the certification to ensure that:

> (1) the certification contains all of the statutorily required elements;
>
> (2) the targeting procedures are reasonably designed to ensure that an acquisition is limited to targeting non-U.S. persons reasonably believed to be located outside the United States;
>
> (3) the targeting procedures are reasonably designed to prevent the intentional acquisition of communications known at the time of acquisition to be wholly domestic;
>
> (4) the minimization procedures are reasonably designed in light of the purpose and technique of the particular surveillance to minimize the acquisition and retention of—and prohibit the dissemination of—information concerning nonconsenting United States persons that is not publicly available, consistent

> with the needs of the government to obtain, produce, and disseminate foreign intelligence information; and
>
> (5) that the certification, and targeting and minimization procedures are consistent with the Fourth Amendment.

See id. § 1881a(d), (i). If the FISC approves the certification and the use of the targeting and minimization procedures, the government may conduct the approved targeting for up to one year. *Id.* § 1881a(a).

Importantly, Section 702 expressly prohibits the intentional targeting of any U.S. person or any person known at the time of acquisition to be in the United States. 50 U.S.C. § 1881a(b).

B. Factual Background: Upstream Collection Under Section 702[1]

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. *See* Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the FISA,* 41-46 (July 2, 2014) (PCLOB Report), Dkt. No. 77-8.[2] Examples of such individuals include members of

[1] The facts in this section are based on documents that were incorporated by reference in plaintiffs' complaint. For purposes of this appeal, these facts are assumed to be true (unless the Court addresses the government's factual challenge, *see infra* pp. 15-20, 43-45).

[2] The Privacy and Civil Liberties Oversight Board is an independent, bipartisan agency within the executive branch that was established by the Implementing

Continued on next page.

foreign terrorist organizations. *See Liberty and Security in a Changing World*: *Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies*, 136 (Dec. 12, 2013) (PRG Report), Dkt. No. 77-9. Next, the NSA identifies a specific means by which the target communicates, such as an e-mail address or telephone number, referred to as a "selector." Selectors must be specific communications identifiers; they *cannot* be keywords or names of targeted individuals. PRG Report 136; PCLOB Report 32-33, 36. The NSA then "tasks" the selector for collection. PCLOB Report 32-33, 36.

The NSA acquires communications associated with tasked selectors using two methods, known as "Upstream" and "PRISM." PCLOB Report 33. Under PRISM collection—not at issue in this case, JA 40—the Government notifies U.S.-based Internet-service providers of tasked selectors, and the providers furnish the NSA with electronic communications to or from these selectors. PCLOB Report 33. In contrast, Upstream involves collection of communications as they transit certain Internet "backbone" networks of U.S. telecommunications-service providers. PCLOB Report 35; PRG Report 141 n.137. Tasked selectors are sent to providers operating these networks, whereupon they must assist the government in intercepting communications to, from, or "about" these selectors (*i.e.,* "about" communications

---

Recommendations of the 9/11 Commission Act of 2007, 42 U.S.C. § 2000ee. It is authorized to review and analyze executive branch actions protecting the Nation from terrorism, to ensure that the need for such actions is balanced against the need to protect privacy and civil liberties.

are ones that contain a tasked selector, such as an e-mail address, in their content). PCLOB Report 36-37; *see also* 50 U.S.C. § 1881a(h). This process "may require access to a larger body of international communications than those that contain a tasked selector." PCLOB Report 111 n.476. But "the government has no ability to examine or otherwise make use of this larger body of communications, except to promptly determine whether any of them contain a tasked selector." *Id.* That process is accomplished by a filtering mechanism that is designed to prevent the acquisition of wholly domestic communications and communications that do not contain the relevant selectors. *Id.* 37. Only communications that pass through both filters are acquired and stored in the NSA's databases. *Id.*[3] Further operational details remain classified, including exactly how the filtering is accomplished.

Once communications are acquired, they are subject to FISC-approved minimization procedures. For example, such procedures prohibit the NSA from using U.S. person identifiers, such as e-mail addresses or telephone numbers, to query Internet communications collected under Upstream. PCLOB Report 56-57.

[3] Although Upstream collection is intended to acquire online communications, "it does so through the acquisition of Internet *transactions*" (*i.e.,* "any set of data that travels across the Internet together such that it may be understood by a device on the Internet"). PCLOB Report 39. An Internet transaction may consist of a single discrete communication (such as an e-mail message) to, from, or "about" a tasked selector, or it may contain multiple discrete communications, not all of which are to, from, or "about" a tasked selector. *Id.* In 2011, about ninety percent of the transactions acquired by NSA through Upstream collection were single communication transactions. *Id.*

Moreover, Internet communications acquired through Upstream must generally be aged off NSA systems within two years. *Id.* 60. The agency must also immediately purge any communication determined to be of, or concerning, a U.S. person if it does not contain foreign-intelligence information. *Id.* 61-62.

Upstream collection is a valuable component of the Section 702 intelligence program, which "is critically important to maintaining our national security." H.R. Rep. No. 112-645, pt. 2, at 3, 5; S. Rep. No. 112-174, at 2 (2012); *see also* PCLOB Report 2, 104-10, 124. Information obtained from surveillance under Section 702 has generated insights into the "membership, leadership structure, priorities[,] and plans of international terrorist organizations." PCLOB Report 107; *see generally* PRG Report 143-45. It has revealed "previously unknown terrorist operatives" and enabled the disruption of "previously unknown terrorist plots." PCLOB Report 108, 110. And it has helped counter the proliferation of weapons of mass destruction. *Id.*

C. Proceedings Below

1. Plaintiffs' Complaint

Plaintiffs, nine educational, legal, advocacy, and media organizations, filed suit, claiming that Upstream surveillance violates the Constitution and various federal statutes, and seeking declaratory and injunctive relief. JA 84-85. 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," which includes the "approximately 49 international submarine cables" and

high-capacity terrestrial cables "that carry [I]nternet communications into and out of the United States," JA 42-43, 47-48. Plaintiffs allege that because almost all international Internet traffic flows through these cables, the government monitors "chokepoints" where these cables meet. JA 47. Plaintiffs allege that Upstream "is intended to enable the comprehensive monitoring of international [I]nternet traffic," allowing the NSA to "cop[y] and review[] substantially all international e-mails and other 'text-based' communications." JA 43.

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) review of the copied communications for targeted 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," which "NSA analysts may read, query, data-mine, and analyze." JA 43-44.[4]

The amended complaint's central allegation is that, "for the NSA to reliably obtain communications to, from, or about its targets," the NSA must "intercept[],

[4] As explained below, plaintiffs allege two discrete injuries concerning their online communications: (1) copying, filtering, and reviewing for selectors, and (2) retention and use. JA 43-44, 52. Plaintiffs also use the term "intercept" in their complaint, *see, e.g.,* JA 46, 47, 49, which we understand to refer to an alleged preliminary step to copying, filtering, and reviewing for selectors.

copy[], and review[] substantially all international text-based communications . . . as they transit telecommunications networks inside the United States." JA 46, 48; *see also* JA 43, 49-50 (NSA must collect substantially all international text-based communications to accomplish its goal of "comprehensive monitoring"). Plaintiffs allege that the government, therefore, "has a strong incentive to intercept communications at as many backbone chokepoints as possible." JA 49-50. They further assert that the government is monitoring "many," or at least seven, chokepoints. JA 50-51.

Plaintiffs also assert that it is "virtually certain" that the NSA is intercepting, copying, and reviewing at least some of Wikimedia's communications because of (1) the "sheer volume" of its international electronic communications, JA 46-47, (Wikimedia engages in more than a trillion such communications each year, JA 56) and (2) the "geographic distribution" of its communications "across the globe," JA 47-48.[5] At the same time, the complaint makes clear that the overwhelming majority of these "communications" refer to data transmissions that occur when an Internet user visits a public Wikimedia website. JA 55-56. Plaintiffs allege that "[g]iven the relatively small number of international chokepoints, the immense volume of [Wikimedia's] communications, and the fact that [Wikimedia] communicate[s] with

[5] Plaintiffs' complaint alleged that all of the plaintiffs have standing on this theory. *See, e.g.,* JA 46-47. On appeal, plaintiffs have narrowed this argument solely as to plaintiff Wikimedia. *See, e.g.,* Br. 24-27.

individuals in virtually every country on earth, [Wikimedia's] communications almost certainly traverse every international backbone link connecting the United States with the rest of the world." JA 48. And for the NSA "to reliably obtain" the communications it seeks, plaintiffs contend that the government "must be" copying and reviewing all international text-based communications on each backbone link it monitors, such that some of Wikimedia's communications would be collected. JA 48-50. Plaintiffs further contend that the volume of Wikimedia's communications means that, under a set of unspecified assumptions, "the odds of the government" intercepting at least one of its communications are "greater than 99.9999999999%." JA 47.

Plaintiffs also allege that they "routinely" communicate over the Internet with non-U.S. persons located abroad, *see, e.g.,* JA 30, 46, 53, 56, 58, 61, and that the individuals with whom they communicate are "likely" to be targeted by the government because those individuals are "believed to have information relevant to counterterrorism efforts." JA 52. Plaintiffs further allege, therefore, that "there is a substantial likelihood" that their communications, once intercepted, "are retained, read, and disseminated," which they contend is a "discrete" injury from the alleged interception, copying, and review of their communications. JA 52.

2. The Government's Motion to Dismiss

The government moved to dismiss the amended complaint for lack of standing, relying on *Clapper* v. *Amnesty International, USA*, 133 S. Ct. 1138 (2013).

Defendants challenged plaintiffs' standing on both facial and factual grounds. As to the facial challenge, the government observed that plaintiffs had failed to allege any concrete facts to support their claim that the NSA collects "substantially all" international electronic communications transiting the United States. The government argued that plaintiffs based their argument not on actual knowledge of Upstream's scope or specific mechanics (information that is classified), but on their speculation that Upstream surveillance *must* be all-encompassing in light of their assumptions about the NSA's "technical abilities and strategic incentives."

The government further argued that plaintiff Wikimedia could not establish standing solely based on the alleged volume of its communications without any context establishing that such volume constitutes a significant portion of Internet traffic so as to permit a reasonable inference that at least some of Wikimedia's communications would be intercepted. In any event, the government asserted that, even if the NSA were intercepting some transmissions between Wikimedia's public websites and online users visiting them, Wikimedia had failed to explain how such interception implicated Wikimedia's privacy interests.

In support of its factual challenge, the government submitted two declarations contesting the accuracy of plaintiffs' technical claims as well as the plausibility of the

inferences they sought to draw.[6] Despite having an opportunity to do so in the trial court, plaintiffs have not contested the facts set out in these two declarations, which are thus unrebutted.[7]

a. Lee Declaration

The government submitted the declaration of Robert Lee, a consultant with more than fifteen years' experience in information security, incident response, and digital forensics, JA 101-02, in order to provide background information on "the way information travels through the high-capacity fiber optic cables comprising the Internet 'backbone.'" JA 102. As Mr. Lee explained, the Internet "backbone" is a network of high-capacity fiber-optic cables, including both terrestrial and submarine fiber-optic cables. JA 106. Each fiber-optic cable "consists of multiple smaller sub-cables housed inside that can each contain up to one thousand silica glass fibers." JA 106. Data on the Internet backbone travels through optical signals, or pulses of light, on those glass fibers. JA 106.

---

[6] The government explained in its motion to dismiss that the district court could consider evidence outside of the pleadings in determining its jurisdiction. *See United States ex rel. Vuyyuru* v. *Jadhav*, 555 F.3d 337, 347-48 (4th Cir. 2009); *Velasco* v. *Gov't of Indonesia*, 370 F.3d 392, 398 (4th Cir. 2004).

[7] Plaintiffs had an opportunity to rebut these declarations after the government moved to dismiss the complaint. But instead of responding to the government's jurisdictional arguments with their own evidence, plaintiffs urged the district court to rule on defendants' facial challenge. *See* Opp'n to Mot. to Dismiss, Dkt. No. 86 (Sept. 3, 2015) at 13-16.

Communications transiting the Internet are typically broken up into separate "packets" that can "travel efficiently" across these fibers. JA 104. "Generally, all of the packets comprising a single communication travel on the same single hair-thin glass fiber." JA 107. Because the packets of a single communication are usually routed on the same fiber, "it would not be necessary, *as a technical matter*, to copy the entire stream of communications carried on every fiber within a sub-cable of a backbone cable to be reasonably certain of obtaining all of the packets constituting a specific communication." JA 107. In addition, "not all packets" that make up a single communication "are necessary to intelligibly assemble its contents." JA 107 n.4. Mr. Lee further explained that it would not be necessary to copy all communications on an entire backbone cable "in order to copy all of the communications traveling across a particular sub-cable within that backbone cable." JA 107.

The Lee declaration also provided background on total Internet use. Mr. Lee stated that there are currently about 3 billion Internet users worldwide. JA 115. According to publicly available information, an estimated 6.21 trillion e-mails are sent per month. JA 117. Mr. Lee explained that Wikimedia's allegation about the volume of its communications would amount to "less than four[]-tenths of one percent (0.34%) of just the monthly traffic carried on the Internet, and would represent a much smaller fraction of the total traffic carried on the Internet each month." JA 117. Mr. Lee also compared the number of web page views on Wikimedia's web sites with page views on the top 50 websites, and found that Wikimedia's monthly volume

of page views "is just 1.8% of the monthly page views of these top 50 sites." JA 120. As a result, Mr. Lee concluded that "[c]omparing the number of Wikimedia's international communications to the total volume of global Internet traffic reveals that Wikimedia's share of that traffic is comparatively small." JA 121.

The Lee declaration also explained the automated and anonymous nature of the online data transmissions that occur when an Internet user views, or downloads information from, a publicly accessible website. JA 104-06, 108-13.

b. Salzberg Declaration

Dr. Salzberg, a statistician who provides statistical sampling, analysis, and review for government and industry, and has served as a statistical expert in courts, JA 87-88, provided a declaration to discuss Wikimedia's assertion (JA 47) that "the odds of the government copying and reviewing at least one of the Plaintiffs' communications in a one-year period would be greater than 99.9999999999%." Dr. Salzberg explained that plaintiffs' calculation is based on three assumptions: (1) there is a 0.00000001% chance that the NSA copies and reviews any one particular communication; (2) the chance of copying and reviewing each communication is the same; and (3) the fact that one communication was or was not copied and reviewed does not affect the chances of whether another communication is or is not copied and reviewed. JA 89. Dr. Salzberg noted that plaintiffs provide no support for any of these assumptions. JA 89-90; *see also* JA 46-47. To the contrary, he pointed out that the latter two assumptions "are inconsistent" with plaintiffs' allegations regarding how

the NSA's interception, copying, and selector review work. JA 95. Specifically, Dr. Salzberg explained that, "[t]o be accurate, the Plaintiffs' calculation requires that the copying and review of communications be like a good statistical survey in that the selection for copying and reviewing is random." JA 94. Dr. Salzberg observed that "[p]laintiffs' assertions about how the process works—through the copying of '*certain* high-capacity cables, switches, and routers' (Compl. ¶ 49)—would mean, if accurate, that the process is, in statistical terms," *not* random.[8] *Id.*

Dr. Salzberg further stated that if any of plaintiffs' assumptions were incorrect—and he noted that "each" was "unsupported by any statistical foundation in the Complaint," JA 89—"then the chances of one of Plaintiffs' communications being copied and reviewed could be far less than 100%." JA 95. Moreover, even if it "is highly probable that at least one communication of one of the nine Plaintiffs[] were copied and reviewed," the "chances" that "*each* of the nine Plaintiffs' communications were copied and reviewed" "could be far smaller." JA 90. Dr. Salzberg concluded, therefore, that it would not be "statistically inconsistent for the

[8] For example, Dr. Salzberg explained that, "even if it is known that on a random day 10% of people in the U.S. carry umbrellas, a survey done in Phoenix on a sunny summer day is unlikely to yield any people with umbrellas while one done in Seattle on a rainy winter day is likely to yield many." JA 93. "The assumptions the Plaintiffs use would say that if 1,000 are surveyed, then there is a greater than a 99.9999999999% chance someone surveyed will be carrying an umbrella without regard to whether the survey was in Seattle or Phoenix." JA 93-94.

NSA to have reviewed a very large number of communications but still have reviewed none of the Plaintiffs' communications." JA 90.

3. The District Court's Decision

The district court dismissed plaintiffs' complaint for lack of Article III standing. The court found it unnecessary to address the government's factual evidence because, even assuming the truth of plaintiffs' jurisdictional allegations, plaintiffs' theories of standing were speculative and therefore foreclosed by the Supreme Court's decision in *Amnesty International*. JA 183.

The district court observed that plaintiffs' central claim of injury—that the NSA was intercepting, copying, and reviewing "substantially all" international electronic communications transiting the United States, including theirs—rested on "suppositions and speculation about how Upstream surveillance *must* operate in order to achieve the government's 'stated goals.'" JA 191. Although the district court found it to be a "possibility" that Upstream functions in the manner plaintiffs allege, the court concluded that plaintiffs had failed to plead any "factual matter" to elevate that claim "above a speculative level." JA 191-92. Thus, the court found that "plaintiffs provide no factual basis that the NSA is actually intercepting communications at all chokepoints," JA 191, and concluded that plaintiffs' "'bare assertion[s]'" do not establish standing. JA 192 (citing *Ashcroft* v. *Iqbal*, 556 U.S. 662, 681 (2009)). The court reasoned that "plaintiffs' reliance on the government's capacity and motivation to collect substantially all international text-based Internet

communications is precisely the sort of speculative reasoning foreclosed by [*Amnesty International*]." *Id.*

The district court also rejected plaintiffs' alternative theory that plaintiff Wikimedia has standing because the allegedly large volume and geographic distribution of its claimed communications make it "virtually certain" that the NSA is intercepting at least some of Wikimedia's communications. The court found the analysis undergirding this argument "incomplete and riddled with assumptions." JA 197. The court noted, for example, that plaintiffs had provided "no context for assessing" the relative volume of Wikimedia's communications in comparison to the total volume of Internet communications—a number plaintiffs "d[id] not provide" or "even attempt to estimate." *Id.* "Without defining the universe of the total number of Internet communications, it is impossible to determine whether Wikimedia's alleged one trillion annual Internet communications is significant or just a drop in the bucket of all annual Internet communications." JA 197-98.

The district court also found that plaintiffs "have not alleged facts that plausibly establish that the NSA is using Upstream surveillance to copy all or substantially all communications passing through those chokepoints" that it monitors. JA 199. Instead, "plaintiffs can only speculate, which [*Amnesty International*] forecloses as a basis for standing." *Id.* And, as to plaintiffs' allegation that the odds of one of Wikimedia's communications being intercepted is "99.9999999999%," the court determined that plaintiffs had failed to justify the core assumptions underlying it, and

chided plaintiffs for "dressing" their speculative arguments "in the clothing of mathematical certainty" without any "statistical basis." JA 198 & n.23.

Finally, the court rejected the alternate grounds plaintiffs advanced in support of their standing. First, the district court pointed out that, because "plaintiffs ha[d] not plausibly alleged" that the NSA is even intercepting their communications, they could not logically establish that the NSA "retained, read, or disseminated" those communications. JA 201 n.26. Second, the district court rejected plaintiffs' argument that Upstream surveillance forces them to take burdensome measures to protect the privacy of their Internet communications and chills their First Amendment speech, concluding that those arguments were indistinguishable from the ones rejected by the Supreme Court in *Amnesty International*. JA 201, 202 n.27; *see Amnesty Int'l*, 133 S.Ct. at 1151, 1152 n.7. Third, the court dismissed the alleged injury of plaintiff National Association of Criminal Defense Lawyers—that one of its member's clients had been subject to Section 702 surveillance—finding that "no factual allegations in the [complaint] plausibly establish[ed] that Upstream surveillance" had been used against that client and that "it appears substantially more likely that PRISM collection was used." JA 195.

SUMMARY OF ARGUMENT

The district court correctly dismissed plaintiffs' complaint challenging the legality of the NSA's Upstream surveillance program for lack of jurisdiction because the complaint failed to state a plausible claim of injury sufficient to support plaintiffs'

standing. Plaintiffs' two primary theories of standing—that their international Internet communications are subject to interception because plaintiffs hypothesize that the NSA must collect "substantially all" international text-based communications pursuant to Upstream, and that Wikimedia's Internet communications are subject to interception because they are so numerous and geographically widespread—both rest on speculation as to the scope and scale of Upstream collection, and the means by which that collection is accomplished. But speculation as to how the government's surveillance "must" work under Upstream, in the absence of concrete factual allegations, is insufficient to state a plausible claim of a "certainly impending" injury, as required for Article III standing. The Supreme Court's recent decision in *Amnesty International* makes that conclusion clear.

If there were any doubt as to whether the district court appropriately dismissed plaintiffs' complaint for failure to adequately allege interception of their communications under Upstream, the government's factual evidence supports the district court's analysis and undermines plaintiffs' allegations about how they surmise Upstream surveillance operates. For example, that evidence underscores that the government need not intercept all communications transiting a given chokepoint because, as a technical matter, the government could choose to intercept only communications traveling on a particular sub-cable, or on particular fibers within a sub-cable, as opposed to the entire cable (containing all the sub-cables). That evidence also undermines Wikimedia's assertion that its communications are so

voluminous that they "must" be intercepted. The evidence explains that, in comparison to total Internet traffic, the volume of Wikimedia's communications is not so great as to render it "virtually certain" that the government is intercepting some of its communications.

In any event, even if the complaint plausibly alleged that Wikimedia's communications are being intercepted by Upstream surveillance, the complaint fails to allege how such interception, by itself, causes Wikimedia any actual injury. According to the complaint, the vast majority of these "communications" are data transmissions that occur when an Internet user accesses a public Wikimedia website. Wikimedia has identified no privacy interest of its own in these communications, and it cannot rely on the interests of third parties. Moreover, none of the plaintiffs has alleged how the NSA's claimed interception and filtering of their communications invades a legally cognizable privacy interest so as to state a plausible claim of injury. Under plaintiffs' theory, the NSA temporarily intercepts communications and filters out communications that are not to, from, or do not contain, tasked selectors. In contrast to their alleged injury based on "retention and use" of their communications, plaintiffs do not allege that any NSA analyst or other human reads the content of, or analyzes, those unfiltered, intercepted communications.

Finally, the district court properly concluded that plaintiffs failed to state a plausible injury stemming from the NSA's alleged retention and potential analysis of their international Internet communications. As the district court correctly explained,

because plaintiffs failed to adequately allege the NSA's interception of their communications—a necessary prerequisite to acquisition and retention of those communications—they have not adequately alleged that their communications are retained by the NSA. In any event, plaintiffs can only speculate that the NSA is likely to retain and review *their* communications, given that the targets of surveillance and the categories of foreign-intelligence information authorized for Upstream collection are classified.

STANDARD OF REVIEW

This Court reviews de novo a district court's decision to dismiss for lack of standing. *See Lane v. Holder*, 703 F.3d 668, 671 (4th Cir. 2012).

ARGUMENT

I. PLAINTIFFS FAIL TO ALLEGE THAT THE UPSTREAM PROGRAM IS LIKELY TO INTERCEPT THEIR COMMUNICATIONS.

To withstand a motion to dismiss, a complaint must contain "sufficient factual matter, accepted as true, to 'state a claim to relief 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)). Conclusory allegations and "naked assertion[s] devoid of further factual enhancement" are not entitled to the assumption of truth; only "well-pleaded factual allegations" can "plausibly give rise to an entitlement to relief." *Id.* at 678-79; *see id.* at 680-81. The well-pleaded factual allegations must allow a court to draw a reasonable inference that the claim is plausible for the plaintiff to have

standing. *Id.* at 678-79 ("plausibility" requires "more than a sheer possibility"). The plausibility standard of pleading applies to both the elements of a claim and to the plaintiff's allegations of standing. *David* v. *Alphin*, 704 F.3d 327, 333 (4th Cir. 2013).

To establish Article III standing, which is a threshold jurisdictional requirement for a court to entertain the suit, 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." *Clapper* v. *Amnesty Int'l*, 133 S. Ct. 1138, 1147 (2013). "Although imminence is concededly a somewhat elastic concept," the "threatened injury must be *certainly impending* to constitute injury in fact." *Id.* "'[A]llegations of *possible* future injury' are not sufficient." *Id.* Plaintiffs bear the burden of establishing standing. *Id.* at 1146.

Notably, the Supreme Court has recently applied these long-standing requirements specifically in the context of FISA Section 702. In *Amnesty International*, six organizations sought declaratory and injunctive relief against surveillance authorized by Section 702, alleging that their work "requires them to engage in sensitive international communications with individuals who they believe are likely targets of surveillance under" Section 702. *Amnesty Int'l*, 133 S. Ct. at 1142. Plaintiffs alleged two injuries: (1) an "objectively reasonable likelihood" that their communications would be intercepted in the future pursuant to Section 702 surveillance, and (2) the costly and burdensome measures plaintiffs were forced to

undertake to avoid the substantial risk of surveillance of their communications. *Id.* at 1143, 1146.

The Supreme Court concluded that neither of plaintiffs' alleged injuries was sufficient to establish standing. *Amnesty Int'l*, 133 S. Ct. at 1155. The Court explained that plaintiffs' theory of standing regarding interception of their communications "relies on a highly attenuated chain of possibilities, [which] does not satisfy the requirement that threatened injury must be certainly impending." *Id.* at 1147-48.[9] The Court noted that plaintiffs "have no actual knowledge of the Government's [Section 702] targeting practices," and "merely speculate and make assumptions about whether their communications with their foreign contacts will be acquired under [Section 702]." *Id.* at 1148. And even if plaintiffs could show an injury, the Court explained that plaintiffs could not show that it is traceable to Section 702, because plaintiffs only speculate that any such surveillance would be under Section 702, as opposed to any other authority. *Id.* at 1148. The Court also rejected plaintiffs'

[9] The Court spelled out the chain of speculations on which plaintiffs' theory of standing relied: "(1) the Government will decide to target the communications of non-U.S. persons with whom [plaintiffs] communicate; (2) in so doing, the Government will choose to invoke its authority under [Section 702] rather than utilizing another method of surveillance; (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy [Section 702's] many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of [plaintiffs'] contacts; and (5) [plaintiffs] will be parties to the particular communications that the Government intercepts." *Amnesty Int'l*, 133 S. Ct. at 1148.

assertion of harm based on measures they had taken to avoid potential NSA surveillance, explaining that, because "the harm [plaintiffs] seek to avoid is not certainly impending," plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm." *Id.* at 1151.

The Supreme Court further emphasized 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 was unconstitutional," particularly "in the fields of intelligence gathering and foreign affairs." 133 S. Ct. at 1147.

A. Plaintiffs Do Not Allege A "Certainly Impending" Injury Based On Interception, Copying, And Selector Review Of Their Internet Communications.

Plaintiffs claim that they have been injured by the NSA's Upstream surveillance because they allege that it must intercept, copy, and review for selectors their international text-based communications. Plaintiffs offer two theories as to why they believe such injury is likely: (1) the NSA intercepts, copies, and reviews "substantially all" international text-based communications under Upstream surveillance, to include plaintiffs' communications; and (2) plaintiff Wikimedia participates in a large volume of international communications around the globe such that Upstream surveillance must necessarily include at least some of its communications.

The district court properly concluded that plaintiffs' "allegations depend on suppositions and speculation, with no basis in fact, about how the NSA implements

Upstream surveillance." JA 190. Accordingly, the district court correctly concluded that plaintiffs' standing arguments were foreclosed by *Amnesty International*. JA 192-201.[10]

1. Plaintiffs Cannot Rely On Their Speculative Claim That The NSA Is Intercepting "Substantially All" International Text-Based Communications.

The district court correctly rejected plaintiffs' first theory of standing. As the district court explained, plaintiffs' allegation that the NSA collects "substantially all" international electronic communications rests on "suppositions and speculation about how Upstream surveillance *must* operate in order to achieve the government's 'stated goals.'" JA 191. The district court found that "plaintiffs provide[d] no factual basis that the NSA is actually intercepting communications at all chokepoints." JA 191. And although plaintiffs alleged that the government has the "capacity and motivation to collect substantially all international text-based Internet communications," JA 192, the district court found that plaintiffs had failed to allege any facts concerning the actual scope and scale of Upstream surveillance, JA 191. Indeed, the district court recognized that plaintiffs could not allege such facts "because the scope and scale of Upstream surveillance remain classified." JA 191.

[10] As the district court made clear, it resolved defendants' motion to dismiss as a facial challenge, relying only on the complaint and any documents incorporated by reference. *See* JA 183 n.8. The court's conclusions are confirmed by the government's evidence submitted in support of its factual challenge. *See supra* pp. 15-20; *infra* pp. 43-45.

On appeal, plaintiffs argue that the district court erred in two respects. First, plaintiffs contend (Br. 46-47) that the district court erred in not drawing reasonable inferences in their favor as to how the NSA carries out Upstream surveillance, but instead "credited its own hypothesis about the scope" of the NSA's Upstream collection. The district court did no such thing. The district court properly concluded that, even if plaintiffs' allegations stated a "possibility" of how Upstream collection works, plaintiffs had provided no allegations to show that their theory of how Upstream works was anything other than speculation. JA 191-92. In other words, although plaintiffs alleged that the government could intercept, and had the motivation to intercept, substantially all international text-based communications, plaintiffs alleged no facts to support an inference that the government was, in fact, doing so.

Significantly, the district court recognized that "technical capability is not tantamount to usage levels," and "[p]laintiffs provide no factual basis to support the allegation that the NSA is using its surveillance equipment at full throttle." JA 190-91; *see also Amnesty Int'l*, 133 S. Ct. at 1158-59 (Breyer, J., dissenting) (suggesting that "capacity" to conduct "surveillance of the kind at issue" was relevant to standing, an approach that was rejected by the majority). The district court did not make any finding of its own as to the scope of NSA's Upstream collection; it simply concluded that plaintiffs had failed to allege facts necessary to permit a plausible inference, rather

than speculation, that the NSA "is actually intercepting communications at all chokepoints." JA 191.

Relatedly, plaintiffs take issue with the district court's statement that, because Upstream surveillance must be approved by the FISC, the NSA might not be "using its surveillance equipment to its full potential." JA 191. Plaintiffs contend (Br. 47 & n.17) that the district court concluded that "the FISC had imposed undisclosed limits on the NSA's surveillance," leading the court to conclude that plaintiffs' allegations about the scope and scale of surveillance were incorrect. Plaintiffs, however, misconstrue the district court's reasoning. The district court simply noted that, because Upstream surveillance must be approved by the FISC to ensure that it complies with the Fourth Amendment, 50 U.S.C. § 1881a, it was *possible* that the NSA's surveillance might actually be more targeted than plaintiffs allege. JA 191; *see also Amnesty Int'l*, 133 S. Ct. at 1159 (recognizing that even if NSA has capacity to conduct electronic surveillance as alleged, "the Government must have intelligence court authorization"). The district court did not reach any conclusion of its own about the scope and scale of Upstream surveillance, but simply declined to draw an inference that was not supported by anything other than speculation.

Second, plaintiffs argue (Br. 47) that the district court erred in discounting the NSA's alleged "strong incentive" to engage in comprehensive collection. They contend that the government "must be" comprehensively monitoring international text-based communications in order to accomplish its goal of obtaining all

international communications to, from, and "about" its targets, Br. 40-41, and that this Court "has made clear that motivation matters when assessing plausibility." Br. 47 (citing *SD3, LLC* v. *Black & Decker (U.S.) Inc.*, 801 F.3d 412, 431 (4th Cir. 2015)). *Amnesty International*, however, precludes standing based on such a speculative inference of motive. 133 S. Ct. at 1158-59 (Breyer, J., dissenting) (endorsing view that standing could be based on "capacity" and "motive" for surveillance, which view was rejected by majority); *see also Obama* v. *Klayman*, 800 F.3d 559, 566-68 (D.C. Cir. 2015) (per curiam) (Williams, J., concurring) (claim that surveillance must be comprehensive to achieve government objectives that the government is presumably motivated to attain is insufficient for standing); *id.* at 569-70 (Sentelle, J., dissenting in part). But even putting that aside, plaintiffs present no facts to support that broad assertion. Plaintiffs simply presume that the government has successfully achieved the purported goal, and that the *only* way to successfully attain that goal is to search substantially all text-based communications entering or leaving the country. Br. 43.

This Court's decision in *SD3* v. *Black & Decker (U.S.) Inc.*, 801 F.3d 412 (4th Cir. 2015), is consistent with these principles. In that case, this Court reversed a dismissal of an antitrust complaint for failure to plead an unlawful agreement, concluding that plaintiff "has alleged enough to suggest a plausible agreement to engage in a group boycott." *Id.* at 418. A claim for a conspiracy based on an agreement to restrain trade requires more than merely an allegation of parallel conduct. *Id.* at 424. And this Court concluded that defendants' alleged motivation to

conspire was a relevant circumstantial fact that could support the inference of a conspiracy, *where plaintiff had alleged facts establishing parallel conduct*. *Id.* at 431. *SD3* therefore stands for the unremarkable proposition that motive may be considered in determining whether a complaint states a claim for conspiracy in violation of Section 1 of the Sherman Act. It does not stand for the broad proposition that motive is always relevant in assessing the plausibility of a complaint that lacks plausible factual allegations, or that motivation, by itself, is sufficient to make a claim of injury plausible.

Plaintiffs' brief also highlights certain allegations that they contend state a plausible claim of injury on the theory that NSA collects "substantially all" communications. But these allegations were properly rejected by the district court as insufficient to state a plausible claim for standing.

Plaintiffs claim that to monitor "substantially all" international text-based communications, the NSA need only monitor communications at the chokepoints, and that the NSA has installed surveillance equipment at "many" of the forty-nine chokepoints for such international communications. JA 42, 49-50; *see also* Br. 45-46 (alleging that one telecommunications provider has facilitated surveillance at seven chokepoints). But these facts do not permit a reasonable inference that the NSA is

comprehensively monitoring *all* the chokepoints such that Upstream surveillance must be collecting "substantially all" international text-based communications.[11]

Moreover, as the district court noted, plaintiffs also "assume that the fact that Upstream surveillance equipment has been installed at some of the Internet backbone chokepoints implies that the NSA is intercepting all communications passing through those chokepoints." JA 190. But plaintiffs have provided no facts to support such an assumption; instead, they only allege that the NSA's surveillance equipment has the "capability" to intercept all transmissions passing through any monitored chokepoints. JA 48, 190. As the district court noted however, that fact does not permit a reasonable inference that the "NSA is, in fact, using the surveillance equipment to its full potential." JA 190 ("technical capability is not tantamount to usage levels"). But even if it were accurate that the NSA intercepts all communications at the chokepoints that it monitors, that still does not support an inference that the NSA monitors all, or even most, chokepoints, as would be necessary to conclude that the NSA collects "substantially all" communications.

Plaintiffs rely heavily on the PCLOB Report, suggesting that its description of Upstream collection is sufficient to support their theory of standing. But the limited

[11] Plaintiffs also cite a New York Times article asserting that NSA has installed surveillance equipment in at least seventeen Internet hubs. Br. 46 n.16. Even assuming the truth of that article, and that "Internet hubs" refers to the international chokepoints that plaintiffs reference, it is unclear how monitoring seventeen out of forty-nine chokepoints would support an allegation that the NSA is collecting "substantially all" Internet communications.

facts contained in the PCLOB Report do not support a claim that "substantially all" international text-based communications are being intercepted, copied, and reviewed for selectors by the NSA. Indeed, details about Upstream's scope and its scale, which are critical to plaintiffs' theory of standing, remain classified; the PCLOB Report does not reveal those details. Thus, plaintiffs can only speculate about the extent of the NSA's interceptions, but have no factual allegations to support their claim that the NSA is intercepting substantially all text-based communications. *Amnesty International* makes clear that such a speculative and conjectural injury is insufficient to establish Article III standing, especially given that this case concerns the government's actions in the field of foreign intelligence. 133 S. Ct. at 1147-50. Moreover, as plaintiffs themselves acknowledge (Br. 32), the PCLOB Report by itself does not support their theory of standing, which is also dependent upon what they refer to as "scientific and technological principles" governing the way the Internet works (*i.e.*, that the government must intercept and copy all communications on a particular cable). But plaintiffs have provided no factual allegations to support those purported principles.

The other public documents alluded to by plaintiffs (Br. 43) 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. JA 39-40; ODNI, *Statistical Transparency Report Regarding Use of National Security Authorities* 1, 2 (Apr. 22, 2015) (ODNI Report), Dkt. No. 77-10. 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, or organizations were targets of Upstream collection, as opposed to PRISM, which is responsible for the greater portion of collection under Section 702. ODNI Report 1; PCLOB Report 33-34. But even if all 92,707 were targets of Upstream collection, that says nothing about the scale on which Upstream collection is conducted to maintain surveillance on those targets. Thus, it fails to raise a claim above the speculative level that the NSA intercepts, copies, and reviews for selectors all international online communications sent or received in the U.S.

Plaintiffs also rely on a New York Times article (Br. 43-44) reporting that the NSA intercepts "apparently most e-mails and other text-based communications that cross the [U.S.] border." That quoted remark, however, was not the statement of a knowledgeable government official, but supposition by the journalist who wrote the article, and without basis in the facts reported. Media speculation adds nothing to the plaintiffs' own speculation. Plaintiffs also rely on two so-called "NSA documents" published in the press, one a purported NSA slide, and the other not identified at all. Br. 45-46; JA 50-51. Even if they were genuine (which the government neither confirms nor denies), these documents respectively indicate, at most, that the NSA conducts some degree of surveillance at "many" international chokepoints, JA 51, but not at most, or all, of them.

In short, as the district court properly concluded, 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.

2. Wikimedia Has Not Plausibly Alleged That Its Communications Will Be Intercepted.

In the alternative, plaintiffs rely on their allegation that the government must be intercepting, copying, and reviewing for selectors at least some of plaintiff Wikimedia's communications because of the sheer volume and geographic distribution of those communications. *See* Br. 24-25. Specifically, Wikimedia alleges that it participates in more than one trillion international Internet "communications" per year, which primarily consist of automated transmissions of data that occur when Internet users view or download information that is publicly displayed on Wikimedia websites. JA 56. But Wikimedia provides no context for that allegation; it does not allege what percentage or proportion of total international communications Wikimedia's share amounts to. As the district court appropriately recognized, without such information, Wikimedia (and this Court) can only speculate that its more than one trillion communications constitute such a substantial percentage of total communications so as to make it "virtually certain" that at least some of its communications are intercepted, copied, and reviewed through Upstream collection.

JA 197. Moreover, the district court correctly recognized that this theory of standing, like plaintiffs' first theory, still depends on the allegation that the NSA is intercepting and copying substantially all communications passing through the chokepoints that it monitors. JA 199. As the district court previously concluded, plaintiffs can only speculate that the NSA is doing so. *Id.*

Wikimedia alleges that the "odds of the [the NSA] copying and reviewing at least one of [its] communications in a one-year period would be greater than 99.9999999999%." JA 46-47. The district court properly rejected this figure because plaintiffs provided no basis for their underlying assumption in the calculation—that there is a 0.00000001% chance that the NSA will intercept any particular communication. JA 198; *see also supra* pp. 18-20 (discussing government's factual evidence on this point).

Plaintiffs allege that the district court erred in rejecting Wikimedia's theory of standing in four ways: (1) the district court misunderstood the scope of surveillance at issue; (2) the district court rejected plaintiffs' explanation as to why the NSA must copy and review for selectors all international text-based communications on the circuits that it is monitoring; (3) the district court ignored the NSA's own documents, which indicate the NSA is collecting Wikimedia's communications; and (4) the district court misunderstood plaintiffs' statistical example. Each of these arguments lacks merit.

First, the district court acknowledged plaintiffs' point (Br. 31, citing PCLOB Report) that the NSA must filter a "larger body" of communications than those that contain a tasked selector before "it can identify the subset that contain selectors." JA 193. But a "larger body," as referred to in the PCLOB Report, is a nebulous term; it does not say how much larger, and it certainly does not say "all." The PCLOB Report, therefore, does not support plaintiffs' broader speculation (Br. 31-32) that "the NSA must search, at a minimum, all international text-based communications on each circuit it is monitoring."

Second, plaintiffs contend (Br. 32) that the district court erroneously rejected their explanation as to why, "as a technological matter, the NSA must copy and review all the international text-based communications on the circuits it is monitoring." Plaintiffs argue that the district court cannot refuse to draw "inferences and conclusions grounded in scientific and technological principles." Br. 32. But plaintiffs have identified no such scientific or technological principles that would support their essential initial assertion that the NSA "must" copy and review for selectors all communications on the circuits it is monitoring. For example, plaintiffs have not alleged that it is technologically impossible for the NSA to limit its interception to communications transiting certain cables or sub-cables at a given chokepoint, as opposed to the entire cable. *See supra* pp. 16-17 (discussing Lee declaration); *infra* p. 44 (same).

Third, plaintiffs point to a slide (Br. 33-34), which they contend indicates that the NSA is intercepting Wikimedia's communications. The purported "NSA slide" is headed "Why are we interested in HTTP?," and depicts the logos of several well-known websites, including Wikipedia's. Although it makes no reference to Upstream collection or the NSA, Wikimedia interprets this document as "identif[ying] Wikipedia traffic as a target for this kind of surveillance." Br. 33; *see also* JA 63. The Government neither confirms nor denies whether the document is an "NSA slide." But whatever the true provenance and meaning of this slide, Wikimedia has surely misconstrued it. The slide on its face simply observes that the "HTTP" protocol is used in "nearly everything a typical user does on the Internet," and identifies some common Internet web sites, such as Yahoo!, Facebook, Google, and Wikipedia. Moreover, because Wikimedia is a domestic organization located in the United States, JA 31, it is a "person" in the United States under FISA, and the NSA is barred from targeting it for surveillance under Section 702. *See* 50 U.S.C. §§ 1801(m), 1881(a), 1881a(b).[12]

[12] Plaintiffs also rely on another purported NSA document (Br. 33 n.12) to support their claim that the "NSA is intercepting Wikimedia's communications." The government neither confirms nor denies whether the referenced document is an "NSA document." But, whatever it is, the document does not make a single reference to Upstream collection. Plaintiffs' bald assertion that the document shows that the NSA is searching communications intercepted under Upstream surveillance to "identify intercepted Wikimedia communications" is thus pure speculation.

Finally, plaintiffs criticize the district court for misunderstanding their statistical example about the likelihood that Wikimedia's communications are being intercepted. Plaintiffs contend (Br. 36) that their example "was chosen specifically to show what an incomprehensibly small sliver of internet communications the NSA could be surveilling and *still* be virtually certain to copy and review at least one of Wikimedia's communications." But even if Wikimedia's chosen percentage represented a "small sliver of internet communications" (which is far from clear), there is no allegation that such a percentage corresponds to the actual share of Internet communications in which Wikimedia is a participant, as the district court correctly recognized. *See also supra* pp. 18-20 (discussing Salzberg declaration). Accordingly, the district court did not misunderstand their statistical example, but appropriately rejected it as "lack[ing] a statistical basis." JA 198.

Plaintiffs' other arguments on appeal highlight specific allegations that they suggest support Wikimedia's standing. Plaintiffs have, however, failed to identify any error by the district court in rejecting these arguments.

Plaintiffs assert that their communications, because they are allegedly so numerous, traverse every major Internet circuit that carries international communications. Br. 25; JA 48. But plaintiffs provide no support for that assumption. They further contend that, even if the NSA is only monitoring one circuit or chokepoint, the NSA must intercept some of their communications, because "as a technological matter," the NSA "must copy and review all international text-

based communications transiting each of the circuits it monitors." Br. 27. But, as explained above, plaintiffs present no plausible factual allegations to support their assertion that the NSA "must copy and review all international text-based communications" on every circuit it monitors. Nor has the government ever confirmed that the program must operate that way. To the contrary, the scope and scale of the Upstream program remain classified. As the district court explained, therefore, "the 'virtual certainty' plaintiffs allege assumes that the NSA is *actually* using Upstream surveillance in the way plaintiffs suppose is necessary for that mode of surveillance to achieve the NSA's stated goals." JA 199.

Plaintiffs surmise that the NSA must intercept all international communications on a circuit that it monitors "because it is impossible for the agency to know in advance which communications will contain a selector associated with one of its many moving targets." Br. 29. But again, there is no plausible reason to believe the government is so constrained. And even assuming that assumption is true, that does not mean the NSA does, in fact, intercept and copy all international communications on each circuit that it monitors. *See Klayman*, 800 F.3d at 566-68 (Williams, J., concurring); *id.* at 568-70 (Sentelle, J., dissenting in part). "[S]peculat[ion] as to how the [NSA] will exercise [its] discretion in determining which communications to target," and how to target them, is insufficient to establish injury. *Amnesty Int'l*, 133 S. Ct. at 1149.

None of this matters, however, because, as explained below, *see infra* pp. 45-48, even if Wikimedia could plausibly claim that some of its communications were intercepted, copied, and reviewed for selectors under Upstream, it has not alleged any cognizable injury attributable to those actions.

3. Defendants' Declarations Further Support The District Court's Dismissal Of The Complaint.

The district court properly concluded that, on the basis of the complaint (and documents incorporated therein), plaintiffs failed to state a plausible claim for standing. Evidence submitted by the government confirms that plaintiffs failed to plausibly state an injury traceable to the government's alleged interception, copying, and selector review of their communications. As noted above, the government alternatively moved to dismiss plaintiffs' complaint on the basis of two declarations, which demonstrated that the jurisdictional allegations of plaintiffs' complaint were untrue. *See Adams* v. *Bain*, 697 F.2d 1213, 1219 (4th Cir. 1982) (distinguishing between facial and factual motions to dismiss for lack of subject matter jurisdiction). Plaintiffs had an opportunity in the trial court to respond to these declarations, but they failed to do so. Although the district court did not rely on defendants' evidence, concluding that it could resolve the standing issue "on the face of the complaint," JA 183 n.8, that evidence further supports the district court's conclusion that plaintiffs lack standing. Dismissal of the complaint can therefore be affirmed as well on this alternative rationale.

As already described, the key allegations plaintiffs rely on to support their claim of standing based on interception, copying, and review of their communications are that: (1) the NSA must intercept and review substantially all international text-based communications that travel the Internet backbone; and (2) the NSA must intercept and review all communications that transit any chokepoint that it is monitoring in order to obtain all the "packets" of a communication.

The Lee declaration establishes that these assumptions have no basis in fact. As Mr. Lee explains, as a technical matter, the NSA would not need to copy all information on a given cable passing through a chokepoint, nor would it need to copy all communications on every fiber within one of the multiple sub-cables that form the cable "to be reasonably certain of obtaining all of the packets constituting a specific communication." JA 102, 107. Accordingly, plaintiffs' allegation that the NSA "must" intercept, copy, and review substantially all international text-based communications is contradicted by record evidence and cannot support plaintiffs' standing, even if it were otherwise plausible.

In addition, plaintiffs' alternative standing argument, based on the "sheer volume" and "geographic distribution" of Wikimedia's communications relies on at least two unfounded assumptions: (1) Wikimedia's more than one trillion communications constitute a substantial volume of the total Internet communications, and (2) Wikimedia's communications are so voluminous and so geographically widespread that some of them must travel on every circuit. The government's

declarations establish that these assumptions are contrary to the facts. Wikimedia's more than one trillion communications are merely a drop in the bucket of total Internet communications, so as to shatter any alleged certainty that the government must intercept, copy, or review Wikimedia's communications. JA 115-121, JA 90. Similarly, because Wikimedia's communications make up a "comparatively small" share of total Internet traffic, JA 121, and each "backbone" cable consists of multiple sub-cables (each of which in turn contains hundreds of glass fibers that could each independently carry Wikimedia's communications), JA 102, 106, the facts do not support plaintiffs' assumption that Wikimedia's communications must traverse every fiber of every sub-cable such that, if the NSA is monitoring only one fiber or even one sub-cable, it still must be intercepting, copying, and reviewing Wikimedia's communications.

4. Even If Some Of Their Communications Were Likely To Be Intercepted, Plaintiffs Failed To Allege A Cognizable Injury.

Even if plaintiffs' complaint could be construed to state a plausible claim that some of Wikimedia's alleged one trillion online communications are being intercepted, copied, and reviewed for tasked selectors through Upstream surveillance, plaintiff Wikimedia has failed to allege actual injury to itself, as is necessary to establish standing. The "communications" Wikimedia alleges are intercepted are mere Internet "transactions" that lack the hallmarks (and privacy interests) of traditional communications. Indeed, the "communications" Wikimedia relies upon to assert

standing primarily refer to data transmissions that occur when a *user* views or downloads information from one of Wikimedia's public web sites (for which Wikimedia provides only technical infrastructure, not content). JA 54-56. These are no more than automated transmissions of publicly available information displayed on Wikimedia websites, transmissions made at the initiation of anonymous users.

Not surprisingly, Wikimedia does not assert any privacy interest of its own in such communications, but rather asserts a privacy invasion on behalf of the users who access its sites. JA 59 (alleging communications "reveal a detailed picture of the everyday concerns and reading habits of Wikimedia's users"). Thus, even if Wikimedia adequately alleged NSA interception, copying, and selector review of these communications, plaintiffs' complaint alleges no resulting injury except (arguably) to the privacy of Wikimedia's online users.

But even as to those users, it is hard to imagine how Wikimedia could plausibly state a claim that a cognizable privacy interest would be implicated by interception of those transactions, since such a claim would, at a minimum, also require an allegation that the government likely would be able to identify the individual user. Such an allegation would be difficult to support, particularly in light of Wikimedia's acknowledgment (JA 65) that "millions" of its users are unknown even to Wikimedia, and the Lee declaration's explanation of the steps required to identify a user. *See* JA 111 ("when a user simply reads or downloads content from a website, the operators of that site know the public IP address, assigned by an ISP, that is associated with the

particular request from that user's device—but not the identity of the user"), JA 113 ("it is often difficult, and certainly not a trivial matter, to identify the subscriber associated with the public IP address, let alone the individual user who sent the request"), JA 114 ("identifying an individual user who made a particular communication . . . can be a difficult matter").[13] Moreover, Wikimedia's asserted privacy interest on behalf of its users is only implicated if the NSA actually acquires and retains Wikimedia's communications, at the stage where plaintiffs allege that "NSA analysts may read, query, data-mine, and analyze these communications." JA 44. Plaintiffs make no allegation that interception, copy, and review for selectors involves reading or analysis of their communications by an NSA analyst, JA 43, as could potentially implicate the privacy concerns raised by Wikimedia.

Indeed, plaintiffs' complaint generally fails to state a cognizable injury because, whatever the nature of the particular communications at issue, plaintiffs have made no allegation that interception, copying, and filtering for selectors involve any human review of the content of those communications. JA 42-44 (alleging that interception, copying, and selector review involves use of "surveillance devices," but that retention involves the participation of "NSA analysts" to "read" or "analyze" their communications). And, as noted above, the government cannot make any use of initially intercepted communications, except to pass them through a filtering

[13] In any event, for the reasons explained *infra* pp. 56-57, Wikimedia lacks standing to assert third-party interests.

mechanism. PCLOB Report 111 n.476 ("the government has no ability to examine or otherwise make use of this larger body of communications, except to promptly determine whether any of them contain a tasked selector"); *id.* 37. Only communications that pass through both filters (to screen out wholly domestic transactions and those that do not contain a tasked selector) are acquired and stored in the NSA's databases for possible analysis, review, or retention. *Id.* 37. Nor do plaintiffs allege that interception, copying, and filtering interfere in any way with their communications.

B. Plaintiffs Have Not Alleged That Retention And Potential Analysis Of Their Communications Is A "Certainly Impending" Injury.

Plaintiffs allege in the alternative that "there is a substantial likelihood" that the NSA "retains" their intercepted communications, Br. 59, and that such retention inflicts a "discrete injury" upon them. *Id.* 60-61 n.21. The district court properly rejected this theory of standing too.

As the district court recognized, plaintiffs' theory of standing based on retention of their communications fails at the outset because it is even more speculative than their first theory. Regardless of whether such retention and potential analysis would constitute a constitutionally cognizable injury-in-fact, plaintiffs failed to plausibly claim that such an injury is "certainly impending." Because plaintiffs have not plausibly alleged that the government is intercepting their communications through the Upstream program, for the reasons set forth above, it necessarily follows

(as the district court explained) that plaintiffs "have not adequately alleged that any of their communications are retained, read, or disseminated by the NSA" as a result of Upstream collection. JA 201 n. 26.

Even assuming that plaintiffs' communications are being intercepted, copied, and filtered for selectors under Upstream, plaintiffs still lack standing. That is because they have alleged no well-pleaded facts to support their assumption that any of their communications would survive the filtering process and be retained, the essential predicate of their claim that the NSA is "reasonably likely" to review, read, or disseminate any of their communications. The government has not publicly disclosed its targets under the program or the particular categories of foreign-intelligence information it is authorized to acquire. *See* PCLOB Report 24-25 & n.70. Plaintiffs' allegations that they communicate with people "whom the government is *likely to target*," and that a "significant amount of the information" in those communications "is 'foreign intelligence information,'" therefore, are speculative and are not entitled to the presumption of truth. JA 52 (emphasis added).

In any event, the Supreme Court has already rejected plaintiffs' theory that an "objectively reasonable likelihood" of retention, reading, or dissemination is sufficient to confer standing for Article III purposes. *See Amnesty Int'l*, 133 S. Ct. at 1147 (holding that a threatened injury must be "certainly impending" to confer standing, and rejecting the "objectively reasonable likelihood" of injury standard as insufficient). The *Amnesty International* plaintiffs alleged that, "[b]ecause of the nature of their

communications and the identities . . . of the individuals with whom they communicate, plaintiffs reasonably believe that their communications will be . . . retained[] and disseminated" under Section 702 surveillance. *See, e.g.*, ACLU Mem. in Supp. of Pls.' Mot. Summ. J. at 11, *Amnesty Int'l* v. *McConnell*, No. 08-cv-6259, Dkt. No. 7 (S.D.N.Y. filed Sept. 12, 2008). The Supreme Court held those allegations to be "necessarily conjectural" because plaintiffs had "no actual knowledge" of the government's "targeting practices." *Amnesty Int'l*, 133 S. Ct. at 1148-49. That holding bars plaintiffs' indistinguishable claim here.

Plaintiffs resist this conclusion by arguing (Br. 59) that the fact that Upstream surveillance extends to "about" communications (that is, those communications that contain a tasked selector, such as a specific e-mail address) suggests that the NSA might retain communications of "innocent third parties . . . if those communications happen to contain a targeted selector." This argument suffers from the same flaws. First, plaintiffs can only speculate that their communications could be to, from, or contain a tasked selector such that collection of their communications would even be authorized under the Upstream program. Second, as explained above, as a practical matter, the NSA can only retain a communication if the NSA has first intercepted and acquired it. And for all the reasons explained above, plaintiffs have failed to adequately allege that the likelihood that their communications will be intercepted is "certainly impending."

II. Plaintiffs' Arguments As To Why *Amnesty International* Is Inapplicable Are Wrong.

Plaintiffs contend that the district court erred in applying *Amnesty International* to dismiss their complaint. Br. 50-53. The district court addressed, and properly rejected, each of plaintiffs' alleged distinctions.

Plaintiffs claim that the surveillance here is "fundamentally different" from the surveillance in *Amnesty International* because it involves "about" surveillance, which plaintiffs liken to a government official opening and reading every piece of mail to determine whether it contains a particular word or phrase, before deciding to retain that piece of mail for potential use. *See, e.g.,* Br. 1-2, 14. As explained above, plaintiffs' assumption that Upstream surveillance involves intercepting, copying, and filtering "substantially all" international text-based communications in order to obtain "about" communications is not supported by any plausible factual allegations. But even if plaintiffs' assumption about the scope of Upstream surveillance were correct, their analogy is inapt. The process of intercepting, copying, and filtering communications through Upstream surveillance, per plaintiffs' allegations, involves the use of "surveillance devices," JA 42, and does *not* involve any NSA analyst or other human reading the contents of the communications, *see* JA 43-44, as in their mail analogy.

The district court, therefore, correctly explained that plaintiffs' assumption that "about" surveillance involves "examining *every* portion of *every* copied

communication" was unsupported by any factual allegations. JA 193. As the court stated, "[u]nlike the hypothetical government agent reading every word of every communication and retaining the information, 'about surveillance' is targeted insofar as it makes use of only those communications that contain information matching the tasked selectors." JA 193. The district court correctly concluded, therefore, that plaintiff's assumption is based on speculation about how Upstream functions.

The district court further explained that "plaintiffs are correct that more is known about the nature and capabilities of NSA surveillance than was known at the time of [*Amnesty International*], but no more is known about whether Upstream surveillance *actually* intercepts all or substantially all international text-based Internet communications, including plaintiffs' communications. Thus, although plaintiffs' speculative chain is shorter than was the speculative chain in [*Amnesty International*], it is a chain of speculation nonetheless." JA 192.

Finally, the district court rejected plaintiffs' argument that *Amnesty International* is inapplicable because of Wikimedia's role as a plaintiff in this suit. As the court explained, plaintiffs do not allege any facts to show that the volume of Wikimedia's communications is significant relative to total Internet communications, and, in any event, plaintiffs' argument as to Wikimedia's standing still rests on speculation that the NSA is using Upstream to collect all or substantially all international text-based communications that transit through the chokepoints that it is monitoring. JA 197-99. As the district court noted, *Amnesty International* "rejected the argument that

standing could be based on a 'very strong likelihood' that the NSA would 'intercept at least some of plaintiffs' communications' based on speculation about the government's 'motivat[ion]' to exercise its 'capacity' for such interception." JA 199 (citing *Amnesty International*, 133 S. Ct. at 1159) (Breyer, J., dissenting). Moreover, as noted above, Wikimedia alleges no injury to its own privacy interests.

III. The District Court Properly Rejected Plaintiffs' Other Asserted Bases for Standing.

A. *Amnesty International* Forecloses Plaintiffs' Argument That They Have Been Compelled to Take Measures To Avoid Surveillance.

Plaintiffs allege (Br. 55) that they have been forced to take "burdensome and costly measures" to avoid Upstream surveillance, which they argue constitutes an injury-in-fact sufficient to confer standing. The district court properly concluded that *Amnesty International* forecloses that argument. JA 201-02.

Plaintiffs nevertheless contend (Br. 55-56) that *Amnesty International* is inapplicable because Upstream surveillance "is of a wholly different character" that "involv[es] the bulk copying and review of international text-based internet communications," and that there is a "virtual certainty" that their communications are being copied and reviewed. That argument was correctly rejected by the district court. JA 193-94. *Amnesty International* is indistinguishable on this point. Plaintiffs in that case likewise alleged that there was a substantial likelihood that their communications would be intercepted, which the Supreme Court rejected as speculative, given that the

plaintiffs "ha[d] no actual knowledge of the Government's § 1881a targeting practices." 133 S. Ct. at 1148. Similarly, here, plaintiffs have no actual knowledge of the scope or scale of Upstream, and can only speculate on the likelihood that their communications might be intercepted. Accordingly, just as in *Amnesty International*, plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm." 133 S. Ct. at 1151.[14]

As an example of plaintiffs' alleged measures to avoid Upstream surveillance, plaintiffs invoke (Br. 56-57) the actions of attorney Joshua Dratel, who is one member of plaintiff the National Association of Criminal Defense Lawyers ("NACDL"). Mr. Dratel allegedly has "employ[ed] burdensome electronic security measures to protect his communications, and in some instances he has to travel abroad to gather information in person." Plaintiffs contend that such measures are necessary because (1) the government has disclosed that the prosecutions of two of Mr. Dratel's clients were based on information intercepted, acquired, and retained through FISA Section 702 surveillance; and (2) Mr. Dratel's international communications "are especially likely" to have been intercepted and retained "because he is almost certain to have

[14] Nor is Upstream a "bulk" collection program, as plaintiffs allege. Rather, Upstream is designed to acquire only those international text-based communications that are to, from, or otherwise contain targeted selectors. PCLOB Report 111 & n.476 ("the Section 702 program is not based on the indiscriminate collection of information in bulk").

communicated with or about the same foreign individuals" that were the targets of that Section 702 surveillance. *Id.*

The district court properly rejected this argument. Surveillance under Section 702 encompasses both PRISM and Upstream collection, and "[i]n neither of Dratel's cases did the government indicate" whether it derived the information at issue through PRISM or through Upstream, and "it appears substantially more likely that PRISM collection was used in these cases." JA 195. Indeed, as the government has publicly explained, Upstream collection only accounts for about 9% of surveillance under Section 702. PCLOB Report at 33-34. Plaintiffs' allegations thus do not establish that Mr. Dratel, or indeed any member of NACDL, has sustained an injury that is "fairly traceable" to Upstream surveillance. *Amnesty Int'l*, 133 S. Ct. at 1150.

But, even if plaintiffs could plausibly claim that the surveillance of Mr. Dratel's clients was conducted pursuant to Upstream, their claim of injury would nevertheless depend on speculation that Mr. Dratel's international communications "are especially likely to have been not only intercepted but retained—precisely because he is almost certain to have communicated with or about the same foreign individuals" targeted for surveillance. Br. 57. Such speculation is insufficient for standing. *Amnesty Int'l*, 133 S. Ct. at 1148 (rejecting as speculative that "[plaintiffs] will be parties to the particular communications that the Government intercepts"). In light of the fact that tasked selectors are classified, plaintiffs' assertion that their communications are "especially likely" to be to, from, or "about" tasked selectors is unsupported.

B. Plaintiffs Have Not Plausibly Alleged A First Amendment Violation.

Plaintiffs further allege that Upstream surveillance chills their First Amendment rights. Br. 58. The district court also properly rejected this argument based on *Amnesty International*, which recognized that "'[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.'" 133 S. Ct. at 1152 (quoting *Laird* v. *Tatum*, 408 U.S. 1, 13-14 (1972)); *see also* JA 202 n.27.

C. Wikimedia Had Not Plausibly Alleged Standing On Behalf Of Any Third Party.

Finally, plaintiffs contend (Br. 61) that Wikimedia has third-party standing to assert the rights of U.S. persons abroad whose communications with Wikimedia are intercepted and individuals inside the United States whose ability to "exchange information with Wikimedia's foreign readers and editors has been impaired by Upstream surveillance."

Prudential limits on standing provide 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.'" *Kowalski* v. *Tesmer*, 543 U.S. 125, 129 (2004); *Valley Forge Christian Coll.* v. *Americans United for Separation of Church & State*, 454 U.S. 464, 474 (1982); *Doe* v. *Virginia Dep't of State Police*, 713 F.3d 745, 753 (4th Cir. 2013). Consistent with that principle, the district court correctly concluded that plaintiffs

could not rely on third parties' subjective fear of surveillance to state a claim for Article III standing. JA 202.

In any event, Wikimedia has not met any of the requirements for third-party standing: it has not plausibly alleged an Article III injury to itself; it has not asserted a close relationship with the users whose interests it seeks to represent; and it has not identified any practical obstacles to suit by these users. *Freilich* v. *Upper Chesapeake Healthm Inc.*, 313 F.3d 205, 215 (4th Cir. 2002).

CONCLUSION

For the foregoing reasons, the judgment of the district court should be affirmed.

Respectfully submitted,

BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General

DOUGLAS N. LETTER
H. THOMAS BYRON III
MICHAEL SHIH

/s/ Catherine H. Dorsey
CATHERINE H. DORSEY
Attorneys, Appellate Staff
Civil Division, Room 7236
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, D.C. 20530
(202) 514-3469
catherine.dorsey@usdoj.gov

APRIL 2016

CERTIFICATE OF COMPLIANCE

I hereby certify that this brief complies with the requirements of Fed. R. App. P. 32(a)(5) and (6) because it has been prepared in 14-point Garamond, a proportionally spaced font.

I further certify that this brief complies with the type-volume limitation set forth in Fed. R. App. P. 32(a)(7)(B) because it contains 13,515 words, excluding exempt material, according to the count of Microsoft Word.

/s/ Catherine H. Dorsey
CATHERINE H. DORSEY

CERTIFICATE OF SERVICE

I hereby certify that on April 11, 2016, I electronically filed the foregoing brief with the Clerk of the Court for the United States Court of Appeals for the Fourth Circuit by using the appellate CM/ECF system. Participants in the case are registered CM/ECF users, and service will be accomplished by the appellate CM/ECF system.

s/ Catherine H. Dorsey
CATHERINE H. DORSEY

ADDENDUM

TABLE OF CONTENTS

50 U.S.C. § 1881a.....A1

50 U.S.C. § 1881a. Procedures for targeting certain persons outside the United States other than United States persons.

(a) Authorization

Notwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (i)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

(b) Limitations

An acquisition authorized under subsection (a)--

(1) may not intentionally target any person known at the time of acquisition to be located in the United States;

(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;

(3) may not intentionally target a United States person reasonably believed to be located outside the United States;

(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and

(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

(c) Conduct of acquisition

(1) In general

An acquisition authorized under subsection (a) shall be conducted only in accordance with--

(A) the targeting and minimization procedures adopted in accordance with subsections (d) and (e); and

(B) upon submission of a certification in accordance with subsection (g), such certification.

(2) Determination

A determination under this paragraph and for purposes of subsection (a) is a determination by the Attorney General and the Director of National Intelligence that exigent circumstances exist because, without immediate implementation of an authorization under subsection (a), intelligence important to the national security of the United States may be lost or not timely acquired and time does not permit the issuance of an order pursuant to subsection (i)(3) prior to the implementation of such authorization.

(3) Timing of determination

The Attorney General and the Director of National Intelligence may make the determination under paragraph (2)--

(A) before the submission of a certification in accordance with subsection (g); or

(B) by amending a certification pursuant to subsection (i)(1)(C) at any time during which judicial review under subsection (i) of such certification is pending.

(4) Construction

Nothing in subchapter I shall be construed to require an application for a court order under such subchapter for an acquisition that is targeted in accordance with this section at a person reasonably believed to be located outside the United States.

(d) Targeting procedures

(1) Requirement to adopt

The Attorney General, in consultation with the Director of National Intelligence, shall adopt targeting procedures that are reasonably designed to--

(A) ensure that any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

(B) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

(2) Judicial review

The procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (i).

(e) Minimization procedures

(1) Requirement to adopt

The Attorney General, in consultation with the Director of National Intelligence, shall adopt minimization procedures that meet the definition of minimization procedures under section 1801(h) of this title or section 1821(4) of this title, as appropriate, for acquisitions authorized under subsection (a).

(2) Judicial review

The minimization procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (i).

(f) Guidelines for compliance with limitations

(1) Requirement to adopt

The Attorney General, in consultation with the Director of National Intelligence, shall adopt guidelines to ensure--

(A) compliance with the limitations in subsection (b); and

(B) that an application for a court order is filed as required by this chapter.

(2) Submission of guidelines

The Attorney General shall provide the guidelines adopted in accordance with paragraph (1) to--

(A) the congressional intelligence committees;

(B) the Committees on the Judiciary of the Senate and the House of Representatives; and

(C) the Foreign Intelligence Surveillance Court.

(g) Certification

(1) In general

(A) Requirement

Subject to subparagraph (B), prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall provide to the Foreign Intelligence Surveillance Court a written certification and any supporting affidavit, under oath and under seal, in accordance with this subsection.

(B) Exception

If the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2) and time does not permit the submission of a certification under this subsection prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall submit to the Court a certification for such authorization as soon as practicable but in no event later than 7 days after such determination is made.

(2) Requirements

A certification made under this subsection shall--

(A) attest that--

(i) there are procedures in place that have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court that are reasonably designed to--

(I) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

(II) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States;

(ii) the minimization procedures to be used with respect to such acquisition--

(I) meet the definition of minimization procedures under section 1801(h) or 1821(4) of this title, as appropriate; and

(II) have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court;

(iii) guidelines have been adopted in accordance with subsection (f) to ensure compliance with the limitations in subsection (b) and to ensure that an application for a court order is filed as required by this chapter;

(iv) the procedures and guidelines referred to in clauses (i), (ii), and (iii) are consistent with the requirements of the fourth amendment to the Constitution of the United States;

(v) a significant purpose of the acquisition is to obtain foreign intelligence information;

(vi) the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider; and

(vii) the acquisition complies with the limitations in subsection (b);

(B) include the procedures adopted in accordance with subsections (d) and (e);

(C) be supported, as appropriate, by the affidavit of any appropriate official in the area of national security who is--

(i) appointed by the President, by and with the advice and consent of the Senate; or

(ii) the head of an element of the intelligence community;

(D) include--

(i) an effective date for the authorization that is at least 30 days after the submission of the written certification to the court; or

(ii) if the acquisition has begun or the effective date is less than 30 days after the submission of the written certification to the court, the date the acquisition began or the effective date for the acquisition; and

(E) if the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2), include a statement that such determination has been made.

(3) Change in effective date

The Attorney General and the Director of National Intelligence may advance or delay the effective date referred to in paragraph (2)(D) by submitting an amended certification in accordance with subsection (i)(1)(C) to the Foreign Intelligence Surveillance Court for review pursuant to subsection (i).

(4) Limitation

A certification made under this subsection is not required to identify the specific facilities, places, premises, or property at which an acquisition authorized under subsection (a) will be directed or conducted.

(5) Maintenance of certification

The Attorney General or a designee of the Attorney General shall maintain a copy of a certification made under this subsection.

(6) Review

A certification submitted in accordance with this subsection shall be subject to judicial review pursuant to subsection (i).

(h) Directives and judicial review of directives

(1) Authority

With respect to an acquisition authorized under subsection (a), the Attorney General and the Director of National Intelligence may direct, in writing, an electronic communication service provider to--

(A) immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition; and

(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain.

(2) Compensation

The Government shall compensate, at the prevailing rate, an electronic communication service provider for providing information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

(3) Release from liability

No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

(4) Challenging of directives

(A) Authority to challenge

An electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition to modify or set aside such directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.

(B) Assignment

The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section 1803(e)(1) of this title not later than 24 hours after the filing of such petition.

(C) Standards for review

A judge considering a petition filed under subparagraph (A) may grant such petition only if the judge finds that the directive does not meet the requirements of this section, or is otherwise unlawful.

(D) Procedures for initial review

A judge shall conduct an initial review of a petition filed under subparagraph (A) not later than 5 days after being assigned such petition. If the judge determines that such petition does not consist of claims, defenses, or other legal contentions that are warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law, the judge shall immediately deny such petition and affirm the directive or any part of the directive that is the subject of such petition and order the recipient to comply with the directive or any part of it. Upon making a determination under this subparagraph or promptly thereafter, the judge shall provide a written statement for the record of the reasons for such determination.

(E) Procedures for plenary review

If a judge determines that a petition filed under subparagraph (A) requires plenary review, the judge shall affirm, modify, or set aside the directive that is the subject of such petition not later than 30 days after being assigned such petition. If the judge does not set aside the directive, the judge shall immediately affirm or affirm with modifications the directive, and order the recipient to comply with the directive in its entirety or as modified. The judge shall provide a written statement for the record of the reasons for a determination under this subparagraph.

(F) Continued effect

Any directive not explicitly modified or set aside under this paragraph shall remain in full effect.

(G) Contempt of court

Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court.

(5) Enforcement of directives

(A) Order to compel

If an electronic communication service provider fails to comply with a directive issued pursuant to paragraph (1), the Attorney General may file a petition for an order to compel the electronic communication service provider to comply with the directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.

(B) Assignment

The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section 1803(e)(1) of this title not later than 24 hours after the filing of such petition.

(C) Procedures for review

A judge considering a petition filed under subparagraph (A) shall, not later than 30 days after being assigned such petition, issue an order requiring the electronic communication service provider to comply with the directive or any part of it, as issued or as modified, if the judge finds that the directive meets the requirements of this section and is otherwise lawful. The judge shall provide a written statement for the record of the reasons for a determination under this paragraph.

(D) Contempt of Court

Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court.

(E) Process

Any process under this paragraph may be served in any judicial district in which the electronic communication service provider may be found.

(6) Appeal

(A) Appeal to the Court of Review

The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition with the Foreign Intelligence Surveillance Court of Review for review of a decision issued pursuant to paragraph (4) or (5). The Court of Review shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this subparagraph.

(B) Certiorari to the Supreme Court

The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(i) Judicial review of certifications and procedures

(1) In general

(A) Review by the Foreign Intelligence Surveillance Court

The Foreign Intelligence Surveillance Court shall have jurisdiction to review a certification submitted in accordance with subsection (g) and the targeting and minimization procedures adopted in accordance with subsections (d) and (e), and amendments to such certification or such procedures.

(B) Time period for review

The Court shall review a certification submitted in accordance with subsection (g) and the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and shall complete such review and issue an order under paragraph (3) not later than 30 days after the date on which such certification and such procedures are submitted.

(C) Amendments

The Attorney General and the Director of National Intelligence may amend a certification submitted in accordance with subsection (g) or the targeting and minimization procedures adopted in accordance with subsections (d) and (e) as necessary at any time, including if the Court is conducting or has completed review of such certification or such procedures, and shall submit the amended certification or amended procedures to the Court not later than 7 days after amending such certification or such procedures. The Court shall review any amendment under this subparagraph under the procedures set forth in this subsection. The Attorney General and the Director of National Intelligence may authorize the use of an amended certification or amended procedures pending the Court's review of such amended certification or amended procedures.

(2) Review

The Court shall review the following:

(A) Certification

A certification submitted in accordance with subsection (g) to determine whether the certification contains all the required elements.

(B) Targeting procedures

The targeting procedures adopted in accordance with subsection (d) to assess whether the procedures are reasonably designed to--

(i) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

(ii) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

(C) Minimization procedures

The minimization procedures adopted in accordance with subsection (e) to assess whether such procedures meet the definition of minimization procedures under section 1801(h) or section 1821(4) of this title, as appropriate.

(3) Orders

(A) Approval

If the Court finds that a certification submitted in accordance with subsection (g) contains all the required elements and that the targeting and minimization procedures adopted in accordance with subsections (d) and (e) are consistent with the requirements of those subsections and with the fourth amendment to the Constitution of the United States, the Court shall enter an order approving the certification and the use, or continued use in the case of an acquisition authorized pursuant to a determination under subsection (c)(2), of the procedures for the acquisition.

(B) Correction of deficiencies

If the Court finds that a certification submitted in accordance with subsection (g) does not contain all the required elements, or that the procedures adopted in accordance with subsections (d) and (e) are not consistent with the requirements of those subsections or the fourth amendment to the Constitution of the United States, the Court shall issue an order directing the Government to, at the Government's election and to the extent required by the Court's order--

(i) correct any deficiency identified by the Court's order not later than 30 days after the date on which the Court issues the order; or

(ii) cease, or not begin, the implementation of the authorization for which such certification was submitted.

(C) Requirement for written statement

In support of an order under this subsection, the Court shall provide, simultaneously with the order, for the record a written statement of the reasons for the order.

(D) Limitation on use of information

(i) In general

Except as provided in clause (ii), if the Court orders a correction of a deficiency in a certification or procedures under subparagraph (B), no information obtained or evidence derived pursuant to the part of the certification or procedures that has been identified by the Court as deficient concerning any United States person shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired pursuant to such part of such certification or procedures shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of the United States person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(ii) Exception

If the Government corrects any deficiency identified by the order of the Court under subparagraph (B), the Court may permit the use or disclosure of information obtained before the date of the correction under such minimization procedures as the Court may approve for purposes of this clause.

(4) Appeal

(A) Appeal to the Court of Review

The Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of an order under this subsection. The Court of Review shall have jurisdiction to consider such petition. For any decision under this subparagraph affirming, reversing, or modifying an order of the Foreign Intelligence Surveillance Court, the Court of Review shall provide for the record a written statement of the reasons for the decision.

(B) Continuation of acquisition pending rehearing or appeal

Any acquisition affected by an order under paragraph (3)(B) may continue--

(i) during the pendency of any rehearing of the order by the Court en banc; and

(ii) if the Government files a petition for review of an order under this section, until the Court of Review enters an order under subparagraph (C).

(C) Implementation pending appeal

Not later than 60 days after the filing of a petition for review of an order under paragraph (3)(B) directing the correction of a deficiency, the Court of Review shall determine, and enter a corresponding order regarding, whether all or any part of the correction order, as issued or modified, shall be implemented during the pendency of the review.

(D) Certiorari to the Supreme Court

The Government may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(5) Schedule

(A) Reauthorization of authorizations in effect

If the Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a), the Attorney General and the Director of National Intelligence shall, to the extent practicable, submit to the Court the certification prepared in accordance with subsection (g) and the procedures adopted in accordance with subsections (d) and (e) at least 30 days prior to the expiration of such authorization.

(B) Reauthorization of orders, authorizations, and directives

If the Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a) by filing a certification pursuant to subparagraph (A), that authorization, and any directives issued thereunder and any order related thereto, shall remain in effect, notwithstanding the expiration provided for in subsection (a), until the Court issues an order with respect to such certification under paragraph (3) at which time the provisions of that paragraph and paragraph (4) shall apply with respect to such certification.

(j) Judicial proceedings

(1) Expedited judicial proceedings

Judicial proceedings under this section shall be conducted as expeditiously as possible.

(2) Time limits

A time limit for a judicial decision in this section shall apply unless the Court, the Court of Review, or any judge of either the Court or the Court of Review, by order for reasons stated, extends that time as necessary for good cause in a manner consistent with national security.

(k) Maintenance and security of records and proceedings

(1) Standards

The Foreign Intelligence Surveillance Court shall maintain a record of a proceeding under this section, including petitions, appeals, orders, and statements of reasons for a decision, under security measures adopted by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

(2) Filing and review

All petitions under this section shall be filed under seal. In any proceedings under this section, the Court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions of a submission, which may include classified information.

(3) Retention of records

The Attorney General and the Director of National Intelligence shall retain a directive or an order issued under this section for a period of not less than 10 years from the date on which such directive or such order is issued.

(l) Assessments and reviews

(1) Semiannual assessment

Not less frequently than once every 6 months, the Attorney General and Director of National Intelligence shall assess compliance with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f) and shall submit each assessment to--

(A) the Foreign Intelligence Surveillance Court; and

(B) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution--

(i) the congressional intelligence committees; and

(ii) the Committees on the Judiciary of the House of Representatives and the Senate.

(2) Agency assessment

The Inspector General of the Department of Justice and the Inspector General of each element of the intelligence community authorized to acquire foreign intelligence information under subsection (a), with respect to the department or element of such Inspector General--

(A) are authorized to review compliance with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f);

(B) with respect to acquisitions authorized under subsection (a), shall review the number of disseminated intelligence reports containing a reference to a United States-person identity and the number of United States-person identities subsequently disseminated by the element concerned in response to requests for identities that were not referred to by name or title in the original reporting;

(C) with respect to acquisitions authorized under subsection (a), shall review the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and

(D) shall provide each such review to--

(i) the Attorney General;

(ii) the Director of National Intelligence; and

(iii) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution--

(I) the congressional intelligence committees; and

(II) the Committees on the Judiciary of the House of Representatives and the Senate.

(3) Annual review

(A) Requirement to conduct

The head of each element of the intelligence community conducting an acquisition authorized under subsection (a) shall conduct an annual review to determine whether there is reason to believe that foreign intelligence information has been or will be obtained from the acquisition. The annual review shall provide, with respect to acquisitions authorized under subsection (a)--

(i) an accounting of the number of disseminated intelligence reports containing a reference to a United States-person identity;

(ii) an accounting of the number of United States-person identities subsequently disseminated by that element in response to requests for identities that were not referred to by name or title in the original reporting;

(iii) the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and

(iv) a description of any procedures developed by the head of such element of the intelligence community and approved by the Director of National Intelligence to assess, in a manner consistent with national security, operational requirements and the privacy interests of United States persons, the extent to which the acquisitions authorized under subsection (a) acquire the communications of United States persons, and the results of any such assessment.

(B) Use of review

The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall use each such review to evaluate the adequacy of the minimization procedures utilized by such element and, as appropriate, the application of the minimization procedures to a particular acquisition authorized under subsection (a).

(C) Provision of review

The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall provide such review to--

(i) the Foreign Intelligence Surveillance Court;

(ii) the Attorney General;

(iii) the Director of National Intelligence; and

(iv) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution--

(I) the congressional intelligence committees; and

(II) the Committees on the Judiciary of the House of Representatives and the Senate.