IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, *et al.*, *Plaintiffs*, v. NATIONAL SECURITY AGENCY, *et al.*, *Defendants*.	Hon. T. S. Ellis, III Civil Action No. 15-cv-00662-TSE

PLAINTIFFS' MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

Deborah A. Jeon (Bar No. 06905)
David R. Rocah (Bar No. 27315)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838
jeon@aclu-md.org

Patrick Toomey (pro hac vice)
Jameel Jaffer (pro hac vice)
Alex Abdo (pro hac vice)
Ashley Gorski (pro hac vice)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
ptoomey@aclu.org

Charles S. Sims (pro hac vice)
David A. Munkittrick (pro hac vice)
John M. Browning (pro hac vice)
PROSKAUER ROSE LLP
Eleven Times Square
New York, NY 10036
Phone: (212) 969-3000
Fax: (212) 969-2900
csims@proskauer.com

Counsel for Plaintiffs

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

INTRODUCTION

This lawsuit challenges the suspicionless seizure and searching of internet traffic by the National Security Agency ("NSA") on U.S. soil. The NSA conducts this surveillance, called "Upstream" surveillance, by tapping directly into the internet backbone inside the United States—the network of high-capacity cables, switches, and routers that carry vast numbers of Americans' communications with each other and with the rest of the world. In the course of this surveillance, the NSA is seizing substantially all international text-based communications—and many domestic communications as well—and searching the contents of these communications for tens of thousands of search terms. The surveillance exceeds the scope of the authority that Congress provided in the FISA Amendments Act of 2008 ("FAA") and violates the First and Fourth Amendments. Because it is predicated on programmatic surveillance orders issued by the Foreign Intelligence Surveillance Court ("FISC") in the absence of any case or controversy, the surveillance also violates Article III of the Constitution.

Plaintiffs are educational, legal, human rights, and media organizations that collectively engage in more than a trillion sensitive international communications over the internet each year. Plaintiff Wikimedia Foundation ("Wikimedia") communicates with the hundreds of millions of individuals who visit Wikipedia webpages to read or contribute to the vast repository of human knowledge that Wikimedia maintains online. The ability to exchange information in confidence, free from warrantless government monitoring, is essential to each of the Plaintiffs' work. The challenged surveillance violates Plaintiffs' privacy and undermines their ability to carry out activities crucial to their missions.

The government's challenge to the plausibility of Plaintiffs' Amended Complaint should fail. Plaintiffs have plausibly alleged that the government is copying and reviewing substantially

all international text-based communications, including their own. At the very least, they have established to a virtual certainty that the government is copying and reviewing *some* of their communications. The volume of Plaintiffs' communications is so great, the geography of their foreign contacts so diverse, and the routing of internet traffic so varied that their communications almost certainly flow across the major internet backbone circuits the NSA is monitoring. And Plaintiffs' allegations relating to the scope of Upstream surveillance are supported by extensive official government disclosures, detailed technical explanation, credible news reports, and published government documents. To argue that Plaintiffs' Amended Complaint does not satisfy the plausibility standard, as the government does, requires a profound distortion of the pleading requirements.

Perhaps recognizing that it cannot reasonably maintain that Plaintiffs' communications are unlikely to be monitored by the NSA, the government argues that Wikimedia lacks standing because it lacks a protected privacy interest in its communications. This argument is misguided both as a legal matter and a factual one. The interception of Wikimedia's own communications is enough, by itself, to establish Wikimedia's standing. In any event, Wikimedia has demonstrated possessory, privacy, and expressive interests in its communications that are protected by the Fourth and First Amendments.

For these reasons and the others explained below, Plaintiffs respectfully submit that the Court should deny the government's motion.

STATUTORY BACKGROUND

I. The Foreign Intelligence Surveillance Act of 1978

In 1975, Congress established a committee, chaired by Senator Frank Church, to investigate allegations of "substantial wrongdoing" by the intelligence agencies in their conduct

of surveillance. Final Report of the S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities (Book II), S. Rep. No. 94-755, at v (1976) ("Church Report"). The committee discovered that, over the course of decades, the intelligence agencies had "infringed the constitutional rights of American citizens" and "intentionally disregarded" legal limitations on surveillance in the name of "national security." *Id.* at 137. Of particular concern to the committee was that the agencies had "pursued a 'vacuum cleaner' approach to intelligence collection," in some cases intercepting Americans' communications under the pretext of targeting foreigners. *Id.* at 165. To ensure the protection of Americans' communications, the committee recommended that all surveillance of communications "to, from, or about an American without his consent" be subject to a judicial warrant procedure. *Id.* at 309.

In 1978, largely in response to the Church Report, Congress enacted FISA to regulate surveillance conducted for foreign intelligence purposes. The statute created the Foreign Intelligence Surveillance Court ("FISC") and empowered it to review government applications for surveillance in certain foreign intelligence investigations. *See* 50 U.S.C. § 1803(a).

As originally enacted, FISA generally required the government to obtain an individualized order from the FISC before conducting electronic surveillance on U.S. soil. *See id.* §§ 1805, 1809(a)(1). To obtain a FISA order, the government was required to make a detailed factual showing with respect to both the target of the surveillance and the specific communications facility—such as a telephone line—to be monitored. *See id.* § 1804(a). The FISC could issue an order authorizing surveillance only if it found that, among other things, there was "probable cause to believe that the target of the electronic surveillance [was] a foreign power or an agent of a foreign power," and "each of the facilities or places at which the

electronic 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).

The basic framework established by FISA remains in effect today, but it has been modified by the FAA to permit the acquisition of U.S. persons' international communications without probable cause or individualized suspicion, as described below.[1]

II. The Warrantless Wiretapping Program

On October 4, 2001, President George W. Bush secretly authorized the NSA to engage in warrantless electronic surveillance inside the United States. After *The New York Times* exposed the program and a federal district court ruled the program unconstitutional, *ACLU v. NSA*, 438 F. Supp. 2d 754 (E.D. Mich. 2006), the government stated that it would seek authorization from the FISC. One FISC judge authorized the surveillance but another later found it unlawful. *See In re* [*Redacted*], No. [Redacted], at 13–16 (FISC Apr. 3, 2007) (Vinson, J.), http://1.usa.gov/1EljnuE. Subsequently, the government sought legislative amendments to FISA that granted authorities beyond what FISA had allowed for three decades.

III. The FISA Amendments Act of 2008

The legislative amendments sought by the Bush administration were embodied in the FAA.[2] The FAA radically revised the FISA regime by authorizing the government's warrantless acquisition of U.S. persons' international communications from companies inside the United States. Like FISA surveillance, FAA surveillance takes place on U.S. soil. However, surveillance

[1] Throughout this brief, Plaintiffs use the phrase "U.S. persons" to refer to United States citizens and residents. Plaintiffs use the term "international" to describe communications that either originate or terminate outside the United States, but not both.

[2] In August 2007, Congress passed a predecessor statute, the Protect America Act, Pub. L. No. 110-55, 121 Stat. 552 (2007), whose authorities expired in February 2008.

under the FAA is far more sweeping than surveillance traditionally conducted under FISA, and the FAA's implications for U.S. persons' constitutional rights are correspondingly far-reaching.

The FAA allows the government to monitor communications between people inside the United States and foreigners abroad. Specifically, the statute permits the Attorney General and DNI to authorize "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a). No court approves the targets of FAA surveillance—the FISC's oversight role in authorizing FAA surveillance is "narrowly circumscribed." *In re Proceedings Required by § 702(i) of the FAA*, No. 08-01, 2008 WL 9487946, at *2 (FISC Aug. 27, 2008). The FISC's role under the statute consists principally of reviewing the general procedures the government proposes to use in carrying out its surveillance. *See* 50 U.S.C. § 1881a(i). Before obtaining an order, the government must provide to the FISC a written certification attesting that the FISC has approved, or that the government has submitted to the FISC for approval, both "targeting procedures" and "minimization procedures." *Id.* § 1881a(d)–(g). These procedures dictate, at a high level of generality, who may be targeted for surveillance by the executive branch and how communications are to be handled once intercepted. The role that the FISC plays under the FAA bears no resemblance to the role it has traditionally played under FISA or the Fourth Amendment.[3]

Importantly, surveillance conducted under the FAA may be conducted for many purposes, not just counterterrorism. The statute defines "foreign intelligence information" broadly to include, among other things, any information bearing on the foreign affairs of the United States. *Id.* § 1801(e). Moreover, a crucial difference between the FAA and FISA is that the FAA authorizes surveillance not predicated on probable cause or individualized suspicion.

[3] *See, e.g.*, Hearing of the Privacy and Civil Liberties Oversight Bd. ("PCLOB") at 31:27–32:28 (July 9, 2013), http://cs.pn/177IpII (statement of former FISC Judge James Robertson).

When the government submits an FAA application to the FISC, it need not demonstrate that its surveillance targets are agents of foreign powers, engaged in criminal activity, or connected even remotely with terrorism. Rather, the FAA permits the government to target *any* foreigner located outside the United States to obtain foreign intelligence information. Similarly, the FAA does not require the government to identify the specific "facilities, places, premises, or property at which" its surveillance will be directed. *Id*. § 1881a(g)(4). Thus, the government may even direct its surveillance at major internet chokepoints, through which flow the communications of millions of people, rather than at individual telephone lines or email addresses.[4] Because the FAA requires neither particularity nor probable cause, the government can rely on a single FISC order to intercept the communications of countless individuals for up to a year at a time.

To the extent the statute provides safeguards for U.S. persons, the safeguards take the form of "minimization procedures." 50 U.S.C. §§ 1881a(e), 1801(h)(1). The statute's minimization requirements are supposed to protect against the collection, retention, and dissemination of communications that may be intercepted "incidentally" or "inadvertently." Significantly, however, these provisions include an exception that allows the government to retain communications—including those of U.S. persons—if the government concludes that they contain any information broadly considered "foreign intelligence." *Id.* §§ 1801(h), 1801(e). In other words, the statute is designed to allow the government to retain, analyze, and use U.S. persons' communications in investigations.

By dispensing with FISA's principal limitations, the FAA exposes every international communication—that is, every communication between an individual in the United States and a

[4] PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* 36–37 (2014), http://bit.ly/1FJat9g ("PCLOB Report") (incorporated into the Amended Complaint by reference) (Def. Ex. 1)

non-American abroad—to potential surveillance. And as discussed below, the government is using the statute to conduct precisely the kind of vacuum-cleaner–style surveillance that the Church Committee condemned and that the Fourth Amendment was intended to prohibit.

FACTUAL BACKGROUND

I. The Government's Implementation of the FISA Amendments Act

The government has implemented the FAA broadly, relying on the statute to intercept and retain huge volumes of Americans' communications. Am. Compl. ¶ 37. In 2011, FAA surveillance resulted in the retention of more than 250 million communications—a number that does not reflect the far larger quantity of communications whose contents the NSA searched before discarding them. *Id.* ¶¶ 49–50, 62–63.[5] In 2014, the government targeted the communications of 92,707 individuals, groups, and organizations under a single FISC order.[6] Every time a U.S. person communicates with any one of those targets—a target who may be a journalist, academic, or human rights researcher—his or her communications are intercepted and retained. The government has refused to disclose how many U.S. persons' communications it has intercepted or retained under the FAA, but by all indications that number is staggering. *Id.* ¶ 37.

As required by the statute, the government has proposed targeting and minimization procedures and the FISC has approved them. However, although these procedures are ostensibly meant to protect the privacy of U.S. persons, the procedures are weak and riddled with exceptions. By design, they give the government broad latitude to analyze and disseminate U.S. persons' communications—including to search those communications in unrelated criminal investigations for information about Americans. *Id.* ¶¶ 52–54.

[5] *See* [*Redacted*], No. [Redacted], 2011 WL 10945618, at *9–*10 (FISC Oct. 3, 2011); PCLOB Report 111 n.476.

[6] Am. Compl. ¶ 37; ODNI, 2014 Statistical Transparency Report at 1 (Apr. 22, 2015), http://1.usa.gov/1JFUMll (Def. Ex. 3).

The government has acknowledged that it conducts two types of surveillance under the FAA. *See, e.g.*, PCLOB Report 7, 33–41; Def. Br. 9. Under a program called "PRISM," the government obtains stored and real-time communications directly from U.S. companies—such as Google, Yahoo, Facebook, and Microsoft—that provide communications services to targeted accounts. This case concerns a second form of surveillance, called "Upstream" surveillance.

II. Upstream Surveillance

"Upstream" surveillance under the FAA involves the government's warrantless search and seizure of U.S. persons' internet communications as those communications transit networks on U.S. soil. In the course of this surveillance, the NSA seizes Americans' communications en masse and searches the contents of substantially all international text-based communications—and many domestic communications as well—for tens of thousands of search terms.

The government has disclosed a significant amount of information about Upstream surveillance. According to the government, Upstream surveillance entails the monitoring of communications as they travel across the internet "backbone" in the United States. *See* PCLOB Report 35–37; Def. Br. 10. The internet backbone is the network of high-capacity cables, switches, and routers that facilitates both domestic and international communication via the internet. *See* PCLOB Report 35–36; Am. Compl. ¶¶ 41–47. When an individual engages in any kind of internet activity, such as browsing a webpage or sending an email, his computer sends and receives information in the form of data packets that are transmitted along the internet backbone. Once these packets reach their destination, the recipient's computer reassembles the packets to reconstruct the communication. *See* PCLOB Report 125; Am. Compl. ¶¶ 41–46, 66.

The NSA conducts Upstream surveillance using surveillance devices connected to major internet cables, switches, and routers on the internet backbone inside the United States. Am.

Compl. ¶ 47. With the assistance of telecommunications providers, the NSA copies and reviews "text-based" communications—*i.e.*, those whose content includes searchable text, such as emails, search-engine queries, and webpages—for search terms, called "selectors." *Id.* ¶ 48. These selectors include email addresses, phone numbers, IP addresses, and other identifiers that NSA analysts believe to be associated with foreign intelligence targets. *Id.* ¶ 49.

Upstream surveillance can be understood to encompass the following processes, some of which are implemented by telecommunications providers at the NSA's direction:

- **Copying**. Using surveillance devices installed at key access points along the internet backbone, the NSA intercepts and makes a copy of substantially all international text-based communications—and many domestic ones—flowing across certain high-capacity cables, switches, and routers. *Id*.
- **Filtering**. The NSA attempts to filter out and discard some wholly domestic communications from the stream of internet data, while preserving international communications. The NSA's filtering out of domestic communications is incomplete, however—which means that many domestic communications are subject to warrantless surveillance. *Id.*; *see* PCLOB Report 38–41.
- **Content Review**. The NSA reviews the copied communications—including their full content—for instances of its search terms. Again, the search terms are email addresses, phone numbers, IP addresses, and other identifiers associated with the NSA's targets, but those targets need not be suspected terrorists or criminals—they may be journalists, academics, lawyers, or human rights researchers. Am. Compl. ¶¶ 49, 36.
- **Retention and Use**. The NSA retains all communications that contain selectors associated with its targets, as well as those that happened to be bundled with those communications in transit—totaling tens of millions of communications each year.[7] NSA analysts may read and query these communications with few restrictions, and they may share the results with the FBI, including in aid of criminal investigations. *Id.* ¶ 49.

Two aspects of Upstream surveillance bear emphasis. First, Upstream surveillance is not limited to communications sent or received by the NSA's targets. The government has acknowledged that the NSA also engages in what is called "about" surveillance—*i.e.*, that it is systematically searching internet traffic for communications that are merely *about* its targets.

[7] *[Redacted]*, 2011 WL 10945618, at *10 & n.26.

See, e.g., PCLOB Report 7, 37–38, 122. It has acknowledged, in other words, that the NSA intercepts vast quantities of internet traffic and examines the full contents of essentially *everyone's* communications to determine whether they include references to the NSA's search terms. *See, e.g.*, *id.* at 111 n.476; *id.* at 37–38 (acknowledging that the NSA "screens" communications transiting the internet backbone in search of its selectors); Def. Br. 10 (same). This is the digital analogue of having a government agent open every piece of mail that comes through the post to determine whether it mentions a particular word or phrase. Most pieces of mail—or email—will contain nothing of interest, but the government must still look through each one to find out. Although it could do so, the government makes no meaningful effort to avoid the interception of communications that are merely "about" its targets (as opposed to those "to" or "from" its targets); nor does it later purge those communications. *See, e.g.*, PCLOB Report 122; Am. Compl. ¶¶ 50–51.

Second, while the government has discussed the FAA as if it implicates only international communications, Upstream surveillance implicates domestic communications as well. *See, e.g.*, PCLOB Report 38. One reason for this is that the NSA's filters are imperfect, and the NSA sometimes mistakes a domestic communication for an international one. *See id.*; *see also* Am. Compl. ¶¶ 49, 54. Another reason is that the NSA retains communications that happen to be bundled, while in transit, with communications that contain selectors—meaning that, each year, the NSA retains hundreds of thousands of communications that have no relation whatsoever to its targets. *See, e.g.*, PCLOB Report 38–41; *[Redacted]*, 2011 WL 10945618, at *9, *11–16.

III. Plaintiffs' Communications

Collectively, Plaintiffs—educational, legal, human rights, and media organizations—engage in an immense number of internet communications every single day, with individuals

located in virtually every country on earth. Am. Compl. ¶¶ 58, 61, 85, 88. Plaintiffs' work requires them to engage in sensitive and sometimes privileged communications, both international and domestic, with, among others, journalists, clients, experts, attorneys, foreign government officials, victims of human rights abuses, and individuals who are of investigative interest to the U.S. government. *Id*. ¶¶ 55, 104, 115, 125, 133, 138, 143, 148, 153, 158, 163.

As the operator of one of the most-visited websites in the world, Plaintiff Wikimedia alone engages in more than one trillion international internet communications each year. *Id*. ¶ 88. Wikimedia communicates with millions of individuals abroad who read, edit, and contribute to the twelve Wikimedia Projects from nearly every country on earth. *Id*. ¶¶ 6, 85, 88. The best-known of Wikimedia's "Projects" is Wikipedia—a free internet encyclopedia that is one of the largest collections of shared knowledge in human history. In 2014, Wikipedia contained more than 33 million articles in over 275 languages, and collectively the Wikimedia sites received between approximately 412 and 495 million monthly visitors. *Id.* ¶ 79. Wikipedia's content is collaboratively researched and written by millions of volunteers, many of whom choose not to identify themselves, and is in most instances open to editing by anyone. *Id*.

Upstream surveillance implicates at least three categories of Wikimedia communications:

- **Communications of Wikimedia with its community members**. Wikimedia engages in more than one trillion international communications each year with those who read and contribute to Wikimedia's Projects and webpages, and with those who use the Projects and webpages to interact with each other. Many, but not all, of these communications are HTTP or HTTPS "requests" and "responses" required to view, search, log in, edit, or contribute to a Wikimedia webpage. *Id.* ¶ 88–92.

- **Wikimedia's internal "log" communications.** Wikimedia creates and transmits records related to its users' activities on its webpages in order to help it monitor, study, and improve the Projects. In particular, every time Wikimedia receives a request from a person accessing a Project webpage, it creates a corresponding log entry. In May 2015, Wikimedia transmitted more than 140 billion logs from its servers abroad to its servers in the United States. *Id.* ¶ 93.

- **Communications of Wikimedia staff.** Wikimedia's staff communicate daily with individuals around the world in order to carry out the organization's mission. Their international contacts include foreign government officials, telecommunications companies, legal counsel, project partners, and volunteers. *Id.* ¶¶ 102, 104.

Wikimedia's communications are essential to its organizational mission, as is its ability to protect the privacy of these communications. *Id.* ¶ 89.

Because of the information they contain, Wikimedia's communications with its community members, as well as its internal communications related to the study and improvement of the Projects, are especially sensitive and private. *Id.* ¶ 95. They contain information indicating which specific webpages each particular Wikimedia community member is visiting or editing—in other words, who is reading or writing what. *See id.* ¶¶ 89–91, 93. And, as a consequence, they provide a detailed picture of the everyday concerns of Wikimedia's users, and often constitute a record of their political, religious, sexual, medical, and expressive interests. *Id.* ¶ 95. Seizing and searching these communications is akin to seizing and searching the patron records of the largest library in the world.

As an organization, Wikimedia has an acute interest in the privacy of its communications, one on par with that of users themselves. *Id.* ¶ 98. Wikimedia's communications reveal who it exchanges information with—*i.e.*, who has contributed to the Projects or visited them—and they reveal exactly *what* information Wikimedia has exchanged with any individual user. *Id.* They reveal proprietary information about the use of Wikimedia's websites, which Wikimedia logs internally for its own purposes as part of its efforts to study and improve the Projects. *Id.* ¶ 93. And they reveal other private information about Wikimedia's operations, including details about its technical infrastructure, its data flows, and its member community writ large. *Id.* ¶ 99.

Wikimedia's mission and existence depend on its ability to ensure that readers and editors can explore and contribute to the Projects privately when they choose to do so. *Id.* ¶ 98.

Except when editors publicly disclose their IP addresses, these exchanges are not public; they are private interactions between Wikimedia and its community members. *Id.* (Even when editors publicly disclose their IP addresses, some aspects of their exchanges remain private.) Wikimedia takes numerous, costly steps to protect the confidentiality of its communications. *Id.* ¶¶ 100–01. Doing so is vitally necessary to fostering trust with community members and to encouraging the growth, development, and distribution of free educational content. *Id.* ¶ 98.

ARGUMENT

I. Because the government has challenged the plausibility of the Amended Complaint on its face, the government's declarations should be disregarded.

The government challenges the legal sufficiency of Plaintiffs' allegations: it contends that the Amended Complaint does not contain "sufficient factual matter, accepted as true" to "'state a claim [to standing] that is *plausible* on its face.'" Def. Br. 14 (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)) (emphasis added); *see also, e.g.*, *id.* at 3, 4, 13, 14, 16. When evaluating the "plausibility" of a complaint under *Iqbal*, a court must limit its inquiry to the four corners of the complaint and to any documents incorporated by reference. In addition, factual allegations that are specific and detailed must be accepted as true and viewed in the light most favorable to the plaintiff. Here the government challenges the plausibility of Plaintiffs' Amended Complaint but seeks improperly to rely on material beyond the four corners of that document. In accordance with Fourth Circuit law, this Court should disregard the government's declarations.

Because the government's motion is an *Iqbal* challenge to the plausibility of the Amended Complaint on its face, it is a "facial"—as opposed to "factual"—challenge under Rule 12(b)(1). As the Fourth Circuit has explained, there are "two critically different ways in which to present a motion to dismiss for lack of subject matter jurisdiction." *Adams v. Bain*, 697 F.2d 1213, 1219 (4th Cir. 1982). In a facial challenge, the defendant contends that a complaint

"simply fails to allege facts upon which subject matter jurisdiction can be based." *Id.* In that event, a plaintiff is afforded procedural protections analogous to those provided in the Rule 12(b)(6) context: a court must accept the plaintiff's allegations as true if they are specific and non-conclusory, and judicial inquiry is confined to the complaint itself and documents incorporated by reference. *See, e.g., id.*; *Kerns v. United States*, 585 F.3d 187, 192 (4th Cir. 2009); *Beckham v. Nat'l R.R. Passenger Corp.*, 569 F. Supp. 2d 542, 546–47 (D. Md. 2008); *NLRB v. Vista Del Sol Health Servs.*, 40 F. Supp. 3d 1238, 1249-50 (C.D. Cal. 2014) (refusing to consider attorney declaration and exhibits submitted by movant in support of facial 12(b)(1) challenge "because[] when a party makes a facial attack on jurisdiction, the court must accept the factual allegations in the complaint as true"); *Ohio Scrap Corp. v. United States*, No. 3:14-cv-535, 2014 WL 5529917, at *2 (N.D. Ohio Aug. 27, 2014); 2-12 Moore's Federal Practice–Civil § 12.30.[8]

In a factual challenge, by contrast, the defendant contends that the jurisdictional allegations of the complaint are not true. "A trial court may then go beyond the allegations of the complaint . . . [and] consider evidence by affidavit, depositions or live testimony without converting the proceeding to one for summary judgment." *Adams*, 697 F.2d at 1219; *see also, e.g.*, *Kerns*, 585 F.3d at 193. When resolving a factual challenge, the court must satisfy itself that the factual record has been "fully developed" before deciding the motion. *E.E.O.C. v. Alford*, 142 F.R.D. 283, 287 (E.D. Va. 1992); *see also Adams*, 697 F.2d at 1220 (concluding that there were "not sufficient facts developed at the 12(b)(1) hearing to resolve the jurisdictional issue"). In addition to allowing plaintiffs to submit affidavits, declarations, and other evidence, courts

[8] It is an open question whether *Iqbal*'s plausibility requirement applies to a motion to dismiss under Rule 12(b)(1). *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992); *Maya v. Centex Corp.*, 658 F.3d 1060, 1067 (9th Cir. 2011). The answer is immaterial here because Plaintiffs' allegations plainly meet the plausibility threshold.

routinely grant jurisdictional discovery to ensure that the record is fully developed. *See, e.g.*, *Animators at Law, Inc. v. Capital Legal Solutions, LLC*, 786 F. Supp. 2d 1114, 1115 n.2 (E.D. Va. 2011) (Ellis, J.) (describing grant of jurisdictional discovery "to allow consideration of [a] pivotal issue on a more complete record").[9]

Here, the government has made clear that it is challenging the facial plausibility, rather than the truthfulness, of Plaintiffs' allegations. *See, e.g.*, Def. Br. 3, 4, 14, 16. Although the government obliquely refers to Plaintiffs' "misperceptions" about Upstream surveillance, it does not assert that Plaintiffs' allegations are false nor deny that it is intercepting and retaining their communications. Rather, it suggests that Upstream surveillance does not "necessarily" operate in the manner Plaintiffs allege. *See id*. 29–30. From this, the government wrongly contends that certain of Plaintiffs' allegations are "speculative" and "conclusory," and should thus be disregarded under *Iqbal*. *See id*. 17, 29. The government's challenge, in other words, is to the legal sufficiency of the Amended Complaint.[10]

Accordingly, Plaintiffs respectfully request that the Court disregard the government's declarations and the accompanying exhibits. As the Fourth Circuit has instructed, the Court should accept Plaintiffs' detailed and factual allegations as true, and the Court's analysis should

[9] If the Court treats the government's challenge as a factual one, it should resolve the challenge under Rule 56 rather than Rule 12. The Fourth Circuit has made clear that a court should resolve factual challenges under Rule 56 when jurisdictional and merits questions are intertwined, as they are here. *Adams*, 697 F.2d at 1219; *Kerns*, 585 F.3d at 193 (plaintiff should be afforded the "procedural safeguards . . . that would apply were the plaintiff facing a direct attack on the merits"). The question of whether the government is intercepting Plaintiffs' communications plainly goes to the merits of Plaintiffs' challenge to Upstream surveillance.

[10] Even the government's declarations do not fundamentally contest the truth of Plaintiffs' factual allegations, because they do not purport to address the question of whether the government is in fact intercepting or retaining Plaintiffs' communications. *See, e.g.*, Lee Decl. ¶ 13 n.5 (emphasizing that Mr. Lee has "no knowledge of how the NSA conducts the surveillance at issue in this case"); Salzberg Decl. (solely addressing Plaintiffs' statistical illustration). They are intended to make Plaintiffs' allegations appear less "plausible," but the question of plausibility must be assessed on the face of the Amended Complaint.

be limited to the four corners of the Amended Complaint and documents incorporated therein by reference, such as the PCLOB Report. *See Kerns*, 585 F.3d. at 192. Because the government has brought a facial challenge, its factual submissions are not properly before the Court.

If the Court concludes otherwise and treats the government's challenge as a factual one, Plaintiffs are entitled to make their own factual showing. The government is not permitted to have it both ways—that is, to have the benefit of its own facts without submitting to the procedures and obligations that accompany such a factual contest. If the government is making a factual challenge, Plaintiffs must be afforded the opportunity to present declarations and, if necessary, to seek jurisdictional discovery establishing their standing to sue. *See, e.g.*, *id.*[11]

II. Plaintiffs have plausibly alleged the copying and review of their communications.

To establish the Court's jurisdiction, the Amended Complaint must include plausible allegations sufficient to meet the familiar requirements of standing: (1) an injury in fact, (2) a sufficient causal connection between the injury and the conduct complained of, and (3) a likelihood that the injury will be redressed by a favorable decision. *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014). The injury-in-fact requirement is designed to ensure that the plaintiff has a "personal stake in the outcome of the controversy." *Warth v. Seldin*, 422 U.S. 490, 498 (1975). The asserted injury must be "'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Susan B. Anthony List*, 134 S. Ct. at 2341 (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)). Importantly, a plaintiff seeking

[11] Should the Court conclude that the government has presented a factual challenge, Plaintiffs request the opportunity to submit their own declarations and evidence establishing their standing, and to take jurisdictional discovery. Plaintiffs are prepared to offer, among other materials, the declaration of Steven Bellovin, a professor of computer science at Columbia University with decades of experience in the telecommunications industry. Professor Bellovin is prepared to give his expert opinion on Plaintiffs' contention that the government is intercepting Plaintiffs' communications in the course of Upstream surveillance.

prospective relief need only allege a "substantial risk" of harm. *See id.* at 2341 (quoting *Clapper v. Amnesty Int'l, USA*, 133 S. Ct. 1138, 1150 n.5 (2013)).

As explained below, Plaintiffs have met these requirements here.

A. Plaintiffs have plausibly alleged that the NSA is copying and reviewing "substantially all" international text-based communications, including their own.

One of the core allegations in Plaintiffs' Amended Complaint is that the NSA is systematically copying and reviewing "substantially all" international text-based communications, including Plaintiffs'. Am. Compl. ¶¶ 1, 48–50, 56, 69. This well-pled allegation, which is supported by a wealth of detail, is more than sufficient to satisfy the injury-in-fact requirement. *Id*. ¶¶ 47–50, 56–69.

The government argues that Plaintiffs' claim about the scope of Upstream surveillance is a "bare assertion" unaccompanied by factual matter, Def. Br. 17, but this objection is blind to the actual contents of the Amended Complaint. Plaintiffs provide a detailed technical explanation as well as credible media reports that cite the statements of senior intelligence officials. *See, e.g.*, Am. Compl. ¶¶ 47–50, 56–69. As with all non-conclusory, factual allegations in a complaint, these allegations are entitled to the presumption of truth at the pleading stage. *See Owens v. Balt. City State's Attys. Office*, 767 F.3d 379, 385, 388 (4th Cir. 2014).

In particular, the Amended Complaint explains—largely on the basis of official, documented disclosures by the government itself—the technical factors that enable the government to copy and review substantially all international text-based communications, and the strategic imperatives that compel it to do so. It explains:

- That the structure of the internet backbone funnels most communications entering or leaving the United States through a limited number of international chokepoints, Am. Compl. ¶¶ 46, 60;

- That surveillance equipment installed at such backbone chokepoints permits the government "to examine the contents of all transmissions passing through collection devices and acquire those, for instance, that contain a tasked selector anywhere within them," *id.* ¶ 62 (quoting PCLOB Report 122);

- That, in order to identify the tiny fraction of communications to, from, and "about" the NSA's targets as the government has described, *id.* ¶¶ 50–51, the NSA must copy and review the contents of an enormous quantity of transiting communications, *id.* ¶ 62; *see* PCLOB Report 111 n.476;

- That, because the NSA cannot know in advance which internet packets relate to its thousands of moving targets, it must copy and reassemble, at a minimum, all the packets associated with international text-based communications that transit the circuits it is monitoring, Am. Compl. ¶¶ 42, 63–64;

- That the government has a strong incentive to intercept communications at as many backbone chokepoints as possible in order to reliably obtain the communications of thousands of individual targets whose locations it cannot know in advance and whose communications take ever-changing routes into and out of the United States, *id.* ¶¶ 65–66 (quoting PCLOB Report 10, 143).

Plaintiffs' Amended Complaint also cites media accounts that corroborate the claim that the NSA is intercepting substantially all international text-based communications. For example, it cites a *New York Times* account from August 2013 that states, based on a review of NSA documents and interviews with senior intelligence officials, that "the N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border." Am. Compl. ¶ 69 (quoting Charlie Savage, *N.S.A. Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013, http://nyti.ms/1E1nlsi). The *New York Times* report also explains, consistently with the Amended Complaint, why the NSA's Upstream surveillance is so far-reaching:

> Computer scientists said that it would be difficult to systematically search the contents of the communications without first gathering nearly all cross-border text-based data; fiber-optic networks work by breaking messages into tiny packets that flow at the speed of light over different pathways to their shared destination, so they would need to be captured and reassembled.

Compare id., *with* Am. Compl. ¶¶ 62–63; *see Phillips v. LCI Int'l, Inc.*, 190 F.3d 609, 618 (4th Cir. 1999) (on a motion to dismiss, a court may consider newspaper articles that are "integral to and explicitly relied on in the complaint").

Finally, Plaintiffs' Amended Complaint cites NSA documents that further corroborate their core allegations—for example, by showing that the NSA has installed surveillance equipment at many major chokepoints on the internet backbone. Am. Compl. ¶¶ 68–69. One of these NSA documents states that the NSA has established interception capabilities on "many of the chokepoints operated by U.S. providers through which international communications enter and leave the United States." *Id.* ¶ 69. Another shows that just one of those participating providers has facilitated Upstream surveillance at seven major international chokepoints in the United States. *Id.* ¶ 68.

The government observes that the Amended Complaint "cite[s] no statements by Government officials acknowledging that Upstream surveillance involves the collection of all (or substantially all) international online communications transiting the United States." Def. Br. 17. This argument is misguided. Establishing standing to challenge unconstitutional government conduct does not require Plaintiffs to show that officials have already admitted to the allegations in the Amended Complaint. Plaintiffs have offered a wealth of officially acknowledged information about Upstream surveillance that supports their claims, especially when viewed with Plaintiffs' other factual allegations. *See, e.g.*, Am. Compl. ¶¶ 37, 51, 62, 65–66 (incorporating by reference PCLOB Report; [*Redacted*], 2011 WL 10945618; President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World*

(2013), http://1.usa.gov/1be3wsO (Def. Ex. 2)). At the pleading stage, a plaintiff need only plausibly allege that he has suffered an injury—and Plaintiffs here have done that and more.[12]

To give their objections the appearance of substance, the government also criticizes certain statistics cited in the Amended Complaint—but those criticisms are factually misleading. For instance, the government makes much of the fact that, in 2011, Upstream surveillance accounted for only "roughly 25 million" of the 250 million communications "collected" under the FAA. *See* Def. Br. 19. But, though the government does not say it, its reference to "roughly 25 million" communications here is a reference not to the number of communications *copied and reviewed* by the NSA in the course of Upstream surveillance but to the number of communications *retained* by it after that copying and review. *See* PCLOB Report 37. The number of communications copied and reviewed by the NSA is far, far larger, because, as explained above, the NSA must copy and review an enormous number of transiting communications in order to find the tiny fraction that are to, from, or about its targets. *See* Am. Compl. ¶¶ 50, 62–64; PCLOB Report 111 n.476, 122 (analyzing Upstream surveillance based on the government's ability to "examine the contents of *all* transmissions passing through collection devices and acquire those, for instance, that contain a tasked selector anywhere within them" (emphasis added)). The fact that the NSA *retained* "roughly 25 million" communications in 2011 as a result of Upstream surveillance only underscores the plausibility of Plaintiffs' allegations.

[12] The government gestures abstractly towards the possibility that the state secrets privilege might apply to some facts about Upstream surveillance, Def. Br. 4, 32, but numerous facts about Upstream have been officially acknowledged, as discussed above, and in the instant context the state secrets privilege has been preempted by statute, *see* 50 U.S.C. §§ 1806(f), 1881e (a) (preempting state secrets privilege where lawfulness of FISA and FAA surveillance is challenged). In any event, the government should not be permitted to rely on the state secrets privilege without actually invoking it.

The government's effort to downplay the significance of the fact that it has 92,707 FAA targets is also flawed. Def. Br. 18–19. The fact that the NSA has tens of thousands of surveillance targets (some of which are groups with perhaps hundreds or even thousands of members) plainly makes it more plausible that Upstream surveillance of international text-based communications is comprehensive. Am. Compl. ¶¶ 37, 65–66. The communications of so many targets scattered around the world will travel many different routes across the internet backbone, based on the locations of those various targets, their individual movements over time, and changes in network conditions. *Id.* ¶ 66. The packets that make up those communications will be intermingled with those of the general population in the flow of internet traffic. *Id.* ¶¶ 62–63. An intelligence agency that seeks to reliably intercept communications to, from, or about its targets, has a strong incentive to search substantially all international text-based communications entering or leaving the country—which is precisely what government officials told the *The New York Times* the NSA is doing. *Id*. ¶¶ 65–66, 69 (quoting Charlie Savage, *N.S.A. Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013, http://nyti.ms/1E1nlsi).

None of the government's arguments undermine the plausibility of Plaintiffs' core allegations, and some of its arguments actually underscore their plausibility.

B. Plaintiffs have also established to a virtual certainty that the government is copying and reviewing at least some of their communications.

Even if there were uncertainty about the plausibility of Plaintiffs' well-founded allegation that the NSA is copying and reviewing substantially all international text-based communications, Plaintiffs would still have standing to sue. This is because the Amended Complaint also pleads that, *whatever the scope of the NSA's Upstream surveillance*, this surveillance must involve the copying and reviewing of at least *some* of Plaintiffs' communications. Indeed, based on official

disclosures concerning Upstream surveillance, and the scale and geographic distribution of Plaintiffs' communications, it is a virtual certainty that this is so.

As described in the Amended Complaint, the conclusion that the government is seizing and searching at least some of Plaintiffs' communications is well-founded for at least four reasons. *See* Am. Compl. ¶¶ 57–67.[13]

1. The volume of Plaintiffs' communications.

One reason it is virtually certain—and surely plausible—that the NSA has copied and reviewed at least some of Plaintiffs' communications is that Plaintiffs engage in a staggering number of international text-based communications. *Id*. ¶¶ 58–59. In the course of a year, Plaintiff Wikimedia alone engages in more than one trillion international internet communications, exchanging information with individuals in virtually every country on earth. *Id*. ¶¶ 85, 88. As Plaintiffs explain at length, Upstream surveillance could achieve the government's stated goals only if it entailed the copying and review of a large percentage of international text-based traffic. *Id*. ¶¶ 59–66. But even if one assumes (very, very conservatively) that there is only a 0.00000001% chance that any particular international text-based internet communication will be copied and reviewed by the NSA, 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%. *Id.* ¶ 58.

2. The geographic distribution of Plaintiffs' communications.

A second reason it is plausible that the NSA is copying and reviewing at least some of Plaintiffs' communications is that these communications are distributed across the globe. The internet backbone includes the approximately 49 international submarine cables carrying the vast

[13] As noted above, the government's declarations are not properly before the Court. Nevertheless, Plaintiffs address them in Section II.B.6, *infra*.

majority of internet traffic into and out of the United States, as well as the limited number of high-capacity terrestrial cables that carry traffic between the United States and Canada or Mexico. *Id.* ¶ 60. The junctions where these cables meet the domestic backbone are in essence "chokepoints"—because almost all international internet traffic flows through circuits traversing them. The government has acknowledged using Upstream surveillance to monitor communications on more than one "international Internet link" or "circuit" on the internet backbone. *Id.*; [*Redacted*], 2011 WL 10945618, at *15; PCLOB Report 36–37.

Given the immense volume of Plaintiffs' communications and the fact that Plaintiffs communicate with individuals in virtually every country on earth, Plaintiffs' communications almost certainly traverse every major internet circuit connecting the United States with the rest of the world. Am. Compl. ¶ 61. In other words, Plaintiffs' communications traverse every one of the major internet circuits at which the NSA conducts Upstream surveillance. Moreover, the fact that the major internet circuits entering and leaving the United States converge at a relatively small number of international chokepoints makes it even more likely that the NSA is conducting its Upstream surveillance on circuits carrying Plaintiffs' communications.

3. Upstream surveillance requires the mass copying and review of internet communications.

Still another reason to conclude it is plausible that the NSA is copying and reviewing at least some of Plaintiffs' communications has to do with the stated purpose of Upstream surveillance. In order for the NSA to reliably obtain communications concerning its targets as it has said Upstream is intended to do, the government must be copying and reviewing all of the international text-based communications that travel across the circuits that it monitors. This is so for two reasons: (1) the NSA is seeking communications "about" its targets, not just those to or

from those targets; and (2) the communications containing the NSA's tens of thousands of targeted selectors are intermingled with the communications of everyone else, *id*. ¶¶ 50, 62–63.

For these two reasons, the NSA must copy and review all international text-based communications transiting a given circuit in order to reliably identify those of interest. As a technical matter, it cannot know in advance which communications—or even which packets—will contain a selector associated with one of its many moving targets. *Id*. ¶¶ 62–63. Rather, it must first copy and reassemble all the international text-based communications on that circuit, so that it can then examine their contents for any mention of a targeted selector. *Id*; *see* PCLOB Report 36–37, 122 ("Digital communications like email, however, enable one, as a technological matter, to examine the contents of all transmissions passing through collection devices and acquire those, for instance, that contain a tasked selector anywhere within them."). In short, for every backbone circuit that the NSA monitors using Upstream surveillance, the monitoring must be comprehensive for the government to accomplish its stated goals. Accordingly, even if the NSA were conducting Upstream surveillance on only a single internet backbone circuit, it would be copying and reviewing at least those communications of Plaintiffs that traverse that link.[14]

4. Upstream surveillance requires monitoring many backbone chokepoints.

A fourth basis to conclude that the NSA is copying and reviewing at least some of Plaintiffs' communications is that Upstream surveillance could not be effective unless the government were monitoring many backbone chokepoints, not just a small handful of them. Am. Compl. ¶¶ 65–66. The government's descriptions of Upstream surveillance make clear that the government is interested in obtaining, with a high degree of confidence, all international

[14] In fact, the NSA has confirmed that it conducts Upstream surveillance at more than one point along the internet backbone with the compelled assistance of multiple major telecommunications companies. *See, e.g.*, PCLOB Report 35; *see also* Am. Compl. ¶ 69.

communications to, from, and about its targets. For example, the Privacy and Civil Liberties Oversight Board has described the use of Upstream surveillance to collect "about" communications as "an inevitable byproduct of the government's efforts to *comprehensively* acquire communications that are sent to or from its targets." PCLOB Report 10 (emphasis added). And it has said about Upstream surveillance more generally that its "success . . . depends on collection devices that can *reliably* acquire data packets associated with the proper communications." *Id*. at 143 (emphasis added).

If the government's aim is to "comprehensively" and "reliably" obtain communications to, from, and about targets scattered around the world, it must conduct Upstream surveillance at many different backbone chokepoints. Am. Compl. ¶ 66. That is especially so because the communications of individual targets may take multiple paths when entering or leaving the United States. When two people communicate in real-time, for example, the communications they exchange frequently take different routes across the internet backbone, even though the end-points are the same. In other words, in the course of a single exchange, the communications *from* a target frequently follow a different path than those *to* the target. Relatedly, a target's location will vary over time, as will the network conditions that determine a given communication's path. As a result, a target's communications may traverse one backbone circuit or chokepoint at one moment, but a different one later. Because of these variables, Upstream surveillance would be effective only if it were implemented at a number of backbone chokepoints. *Id*. ¶ 66.

5. Documents published in the press corroborate Plaintiffs' claims.

For the four reasons above, Plaintiffs have plausibly alleged that the NSA is copying and reviewing at least some of their communications. This conclusion is corroborated by government documents that have been published in the press. *See id*. ¶¶ 68–69. In addition to news reports

and NSA documents identified above, which describe the overall reach and comprehensiveness of Upstream surveillance, NSA documents also show that the government has expressed a specific intelligence interest in surveilling Plaintiff Wikimedia's communications. *Id*. ¶ 107. One NSA slide describes analysts' ability to learn "nearly everything a typical user does on the Internet" by surveilling HTTP communications—and identifies Wikipedia as a target for surveillance of exactly that kind. *Id.* The slide pertains to a search tool that allows NSA analysts to examine data intercepted via Upstream surveillance. *See id.*

Given this wealth of support, Plaintiffs' allegations are certainly plausible. Indeed, to hold that a party that has alleged injury with reference to official government disclosures, detailed technical explanation, credible news reports, and published government documents has not satisfied the "plausibility" standard would require a profound distortion of the pleading requirements. Neither *Iqbal* and *Twombly* purported to turn those requirements into insuperable hurdles, and subsequent lower court cases have not interpreted these cases in the way that the government does here. *See Owens*, 767 F.3d at 396, 403–04; *Jewel v. NSA*, 673 F.3d 902, 908–10 (9th Cir. 2011) (finding plaintiffs had standing, on a motion to dismiss, to challenge warrantless surveillance of their internet communications).

6. The government's submissions do not undermine Plaintiffs' well-pled allegations.

In an effort to diminish the facial plausibility of Plaintiffs' allegations, the government has submitted two declarations criticizing some of the conclusions above. As Plaintiffs have explained, those submissions are not properly before the Court and should be disregarded. *See* Section I, *supra*. However, even if the Court were to consider them, they would not undermine Plaintiffs' claims. Neither Mr. Lee nor Dr. Salzberg purports to have any knowledge of the scope of Upstream surveillance, or of whether the government is in fact intercepting Plaintiffs'

communications. Neither Mr. Lee nor Dr. Salzberg claims even to have reviewed the voluminous, publicly available materials describing Upstream surveillance. Instead, they provide misleading criticisms of Plaintiffs' allegations by offering opinions and hypotheticals that are entirely divorced from the publicly disclosed facts.[15]

For example, the Salzberg Declaration argues that the statistical illustration in the Amended Complaint, Am. Compl. ¶ 58, is based on a simplified model, but every model is simplified—this is the very definition of a model. The important point is that, even accounting for the assumptions embedded in it, the model shows how unlikely it is that the government's Upstream surveillance does not touch any of Plaintiffs' communications. The model shows that, even if one makes extremely conservative assumptions about the scale of the government's surveillance, it is virtually certain that that surveillance implicates at least *some* of Plaintiffs' trillion or more communications each year. The Salzberg Declaration points out that Upstream surveillance is non-random, *see* Salzberg Decl. ¶ 19, but the properties that make it non-random are, in combination, precisely what make it virtually certain that Plaintiffs are subject to this surveillance. Those properties are: the likelihood that the NSA filters out immense amounts of video traffic as well as domestic communications, Am. Compl. ¶ 59; the limited number of backbone chokepoints, *id*. ¶ 60; the necessity of copying and reassembling all international text-based traffic on a given circuit, *id*. ¶¶ 62–64; the need to monitor a large group of mobile targets, *id*. ¶¶ 65–66; and the fact that Plaintiffs communicate with millions of individuals around the globe, effectively guaranteeing that their communications traverse every major backbone circuit and chokepoint in the United States. *Id*. ¶ 61. Dr. Salzberg does not address this combination of

[15] As noted above, if the Court construes the government's motion as a factual challenge and declines to disregard the Lee and Salzberg Declarations, Plaintiffs request the opportunity to rebut the government's assertions with their own declarations—including that of Professor Steven Bellovin—and, if necessary, through jurisdictional discovery. *See* Section I, *supra*.

properties; as noted, he does not purport to have considered any of the publicly known facts about Upstream surveillance.

Dr. Salzberg's other arguments reinforce Plaintiffs' claims. For instance, Dr. Salzberg questions the assumption that the NSA is collecting one one-hundred millionth of a percent of internet communications, and points out that smaller percentages produce smaller probabilities of interception. Salzberg Decl. ¶ 11. But what is telling is how small that percentage must be before the probability of intercepting Plaintiffs' communications falls significantly: by Dr. Salzberg's own calculations, one is required to assume that the NSA is copying and reviewing only one one-hundred *billionth* of a percent of internet communications. Yet Upstream surveillance could not accomplish its stated goals if the NSA were intercepting such a vanishingly small proportion of internet communications. *See* Am. Compl. ¶¶ 62–66.[16]

Mr. Lee, for his part, takes issue with Plaintiffs' detailed allegation that the government is copying and reviewing all the international text-based communications traversing a given internet backbone circuit, pointing out that the physical submarine cables can contain multiple fibers. Lee Decl. ¶¶ 11–13. But, even so, that does not undermine Plaintiffs' allegations. Mr. Lee focuses on the physical fibers that comprise each cable, but as the PCLOB Report and the FISC's opinion make clear, Upstream surveillance is directed at major internet "circuits" or "links" on

[16] Notably, the Salzberg Declaration is inconsistent with the statistics presented in the Lee Declaration and with the officially acknowledged statistics concerning Upstream surveillance. The NSA has acknowledged retaining 26.5 million communications under Upstream in 2011. [*Redacted*], 2011 WL 10945618, at *26. Meanwhile, Mr. Lee's declaration estimates that approximately 90 trillion text-searchable communications traverse the global internet in a given year. *See* Lee Decl. ¶¶ 27–28, 31–33. Comparing these figures indicates that the NSA is intercepting 0.0000295% of text-based internet communications. That percentage is 3,000 times higher than the percentage Plaintiffs used in their illustration and 3,000,000 times higher than the one Dr. Salzberg hypothesizes. Salzberg Decl. ¶ 11. And importantly, that percentage relies on a significant understatement of the number of communications the government is copying and reviewing each year using Upstream surveillance, because to *retain* 26.5 million communications, the government must first *copy and review* many times that number.

the internet backbone. PCLOB Report 36–37; [*Redacted*], 2011 WL 1094518, at *15; Am. Compl. ¶¶ 60–61. Each of those circuits, which may span multiple fibers in a given cable, carries an enormous amount of traffic between a major U.S. telecommunications provider and a major provider abroad. Mr. Lee does not dispute that the NSA must be intercepting, at a minimum, all international text-based communications transiting each of the major internet backbone *circuits* it is monitoring. *See also* PCLOB Report 36–37, 122. Because Plaintiffs' trillion-plus communications traverse every major internet backbone circuit, the NSA is indeed copying and reviewing their communications. The volume of Plaintiffs' communications is so immense, the geography of their contacts so diverse, and the routing of internet traffic so varied that their communications almost certainly flow across whichever combination of major internet circuits the government is monitoring. Am. Compl. ¶¶ 60–61; *id.* ¶¶ 68–69 (documents showing that the NSA is acting on "many of the chokepoints operated by U.S. providers").

Just as importantly, the Lee Declaration's technical discussion fails to take into account the actual functioning of Upstream surveillance as described by the government. *See* Lee Decl. ¶ 13 n.5 (disclaiming any "knowledge of how the NSA conducts the surveillance at issue in this case."). Mr. Lee suggests that the NSA need not copy the communications traversing multiple fibers within a backbone cable in order "to be reasonably certain of obtaining all of the packets constituting a specific communication." *Id*. ¶¶ 12–13. This might be true if the NSA were seeking "a specific communication" from a single target in a known location, but of course the NSA has not defended Upstream surveillance based on its need to capture any "specific communication," but based on its purported need to capture the millions of communications to, from, and about its thousands or tens of thousands of targets from many regions of the world. At that scale, the NSA could not reliably reassemble the packets of all of the text-based

communications it is targeting without also copying and reassembling the packets of text-based communications carried on all of the fibers that form part of the same major internet circuit. As Mr. Lee himself concedes, while it is "likely" that all of the packets comprising a single communication will travel on the same fiber, that is by no means required. *Compare* Lee Decl. ¶¶ 12–13, *with* PCLOB Report 125 (observing that even a single email "can be broken up into a number of data packets that take different routes to their common destination."). At scale, this matters. Because the NSA is seeking to review the contents of immense quantities of internet communications, its ability to reliably identify those to, from, and about its targets would be significantly impaired if it were not copying and reassembling all the international text-based traffic transiting a given internet backbone circuit.

C. The government's reliance on *Amnesty International* is misplaced.

The government suggests that Plaintiffs' challenge to Upstream surveillance is foreclosed by *Clapper v. Amnesty International, USA*, 133 S. Ct. 1138 (2013), but this case arises in a markedly different factual and legal context than did the suit filed seven years ago. The government's argument depends on distorting both *Amnesty* and Plaintiffs' Amended Complaint.

As an initial matter, the facts before this Court are dramatically different from the ones that were before the Supreme Court in *Amnesty*. While *Amnesty* involved a challenge to the FAA, at the time the case was litigated neither the public nor the Supreme Court knew much about how the statute was being used. The assumption of the *Amnesty* plaintiffs and of the Supreme Court was that the statute was being used to intercept the communications of "targets," but nothing was known about how many targets there were, let alone how the targets' communications were being acquired. *See id.* at 1148. Even more significantly, nothing was known about the NSA's practice of "about" surveillance because the government had not

publicly discussed the practice, the government did not disclose it to the Supreme Court, it had not been the subject of media reports, and it was not contemplated by the plain language of the statute. Am. Compl. ¶¶ 50–51.[17] The Supreme Court's analysis in *Amnesty* was predicated on the theory—now known to be incorrect—that surveillance under the FAA implicated only those who were in direct contact with the NSA's surveillance targets. *See, e.g.*, *Amnesty*, 133 S. Ct. at 1148.

Upstream surveillance—which is the focus of *this* case—came to public attention only after *Amnesty* was decided. Am. Compl. ¶¶ 50–51; *see also* Charlie Savage, *N.S.A. Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013, http://nyti.ms/1E1nlsi. It was only after the Supreme Court decided *Amnesty* that the government disclosed the existence of Upstream surveillance and discussed its contours; that the government released FISC opinions describing Upstream surveillance in some detail; and that the PCLOB examined Upstream surveillance in an extensive public report.[18] It was only after the Supreme Court decided *Amnesty* that the government acknowledged that it was engaged in "about" surveillance—in other words, it was only after *Amnesty* that the government disclosed it was searching the communications of essentially everyone, targets and non-targets alike. Am. Compl. ¶¶ 50–51. Some have argued persuasively that the government should have been more candid with the Supreme Court, *see, e.g.*, Letter from Sens. Ron Wyden, Mark Udall, and Martin Heinrich to Solicitor General Donald Verrilli at 1–3 (Nov. 20, 2013), http://bit.ly/1JcrJDU, but the important fact for present purposes is that it was not.

[17] *See* PCLOB Report 84 ("The fact that the government engages in such collection is not readily apparent from the face of the statute, nor was collection of information 'about' a target addressed in the public debate preceding the enactment of FISA or the subsequent enactment of the FISA Amendments Act" in 2008).

[18] *See, e.g.*, PCLOB Report (citing FISC opinions, public hearings and testimony by intelligence officials, executive-branch compliance assessment, statistical transparency report, privacy report, and FAA minimization procedures).

The government argues that *Amnesty* controls here but it does not actually engage with *Amnesty's* reasoning, which was very much tied to the factual record that the Supreme Court had before it. In concluding that the plaintiffs lacked standing, the Supreme Court cited the plaintiffs' inability to show that the government had sought FISC authority to engage in the surveillance they challenged, that the FISC had granted the authority, or that their communications would be implicated by the surveillance. 133 S. Ct. at 1148. Here, by contrast, it is clear that the government is engaged in the surveillance that Plaintiffs challenge—the government has acknowledged the surveillance and described it in detail. It is also clear that the FISC has authorized this surveillance. *See, e.g.*, [*Redacted*], 2011 WL 10945618. And, because of the nature of the surveillance, it is clear that Plaintiffs' communications are implicated by it. This last point bears emphasis. Again, *Amnesty* was litigated on the premise that the government was intercepting the communications of *targets*, and accordingly the question the Court asked was whether the Plaintiffs had shown a sufficient likelihood that their contacts were targets. Now, however, it is plain that the government has *tens of thousands* of targets, Am. Compl. ¶ 37—and that it is copying and reviewing the communications *of essentially everyone* in order to find communications to, from, and *about* those many targets. *Id.* ¶¶ 50–51; PCLOB Report 111 n.476. In *Amnesty*, the Supreme Court held that it was not clear the FISC had authorized surveillance under the FAA *at all*, let alone that it was likely that the plaintiffs' communications would be implicated by the surveillance. Here, Plaintiffs have alleged, in detail and with extensive corroborating support, that the NSA is in fact copying and reviewing their communications. Am. Compl. ¶¶ 56–69.

This case is also in a different procedural posture than *Amnesty*, which was decided on a motion for summary judgment. *See* 133 S. Ct. at 1146. Here, the government asked the Court to

defer consideration of summary judgment motions so that the government could first challenge Plaintiffs' standing on the face of the pleadings. *See* Def. Mot. to Set Status Conf. (ECF No. 54). The question in *Amnesty* was whether the plaintiffs were entitled to judgment as a matter of law. Here, Plaintiffs need only show that their allegations establishing standing are plausible.

Finally, the government is wrong to contend that *Amnesty* established a new, higher standing threshold. The Court observed in *Amnesty* that it had previously held that a plaintiff establishes an injury in fact by demonstrating a "substantial risk" of injury, and the Court did not disavow those precedents. 133 S. Ct. at 1150 n.5 (citing, *e.g.*, *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 153–55 (2010)). Moreover, the Supreme Court reaffirmed the "substantial risk" standard just last year. *Susan B. Anthony List*, 134 S. Ct. at 2341. The pleadings here easily surmount this threshold. Plaintiffs have presented specific details about the immense volume and worldwide distribution of their international communications, and they have set those facts alongside a technical description of how and why the government is copying and reviewing substantially all international text-based communications traversing the internet backbone. Am. Compl. ¶¶ 47–50, 56–69. They have made precisely the kind of showing that the Supreme Court found the plaintiffs had not made in *Amnesty*.

III. The government's copying and review of Plaintiffs' communications establishes standing.

A. To establish standing, Plaintiffs need show only that the government has intercepted their communications.

Plaintiffs' well-pled allegation that the government is intercepting their communications establishes their standing to sue. The interception of Plaintiffs' communications is an injury in fact that satisfies the requirement that a plaintiff have a "personal stake in the outcome of the controversy." *Warth*, 422 U.S. at 498. Moreover, Plaintiffs have described in detail their privacy,

possessory, and expressive interests in the communications the government is intercepting. *See, e.g.*, Am. Compl. ¶¶ 55, 73, 76, 89–95, 98–99, 113, 118, 131, 134. In other words, Plaintiffs' asserted injury is "concrete and particularized," it is fairly traceable to Upstream surveillance, and it would be redressed by the relief they seek. *Susan B. Anthony List*, 134 S. Ct. at 2342. They need not allege more in order to establish the Court's jurisdiction. *See ACLU v. Clapper*, 785 F.3d 787, 801 (2d Cir. 2015); *Amidax Trading Grp. v. S.W.I.F.T. SCRL*, 671 F.3d 140, 147 (2d Cir. 2011) (observing, in dicta, "[t]o establish an injury in fact—and thus, a personal stake in this litigation—[plaintiff] need only establish that its information was obtained by the government").

The government argues that Wikimedia does not have standing to prosecute this suit even if it has plausibly alleged the interception of its communications, because (in the government's view) Wikimedia has not alleged a privacy interest of its own in some of the communications the NSA is copying and reviewing. Def. Br. 34–37.[19] The government is wrong. As an initial matter, the government does not contest that Wikimedia has a possessory and expressive interest in these communications, *see id.*, so nothing turns on whether Wikimedia has a privacy interest in them. But Wikimedia *does* have a privacy interest in them. *See, e.g.*, Am. Compl. ¶¶ 89–95, 98–99. Whether that privacy interest is one *protected by the Fourth Amendment* is a distinct question—and, as the Supreme Court has made clear, it is a merits question. Indeed, insofar as the government argues that Wikimedia lacks standing because the interception of its own communications does not amount to an injury to Wikimedia's privacy rights, Def. Br. 37, the government conflates the standing inquiry with the substantive constitutional one. *See, e.g.*, *Rakas v. Illinois*, 439 U.S. 128, 139–40 (1978) (stating that the definition of Fourth Amendment

[19] The government does not raise this objection as to any of the other Plaintiffs. Nor does the government raise this objection with respect to all of Wikimedia's communications, as explained below. *See Section* III.B, *infra*.

rights "is more properly placed within the purview of substantive Fourth Amendment law than within that of standing"); *Minnesota v. Carter*, 525 U.S. 83, 88 (1998) (criticizing courts for analyzing whether a party has "a legitimate expectation of privacy" under "the rubric of 'standing' doctrine"); *United States v. Lawson*, 410 F.3d 735, 740 n.4 (D.C. Cir. 2005).

The government also argues that Wikimedia lacks standing to challenge surveillance of even its *internal* "log" communications reflecting users' activities—purportedly because any privacy interest in those communications belongs to Wikimedia's community members, not to Wikimedia itself. Def. Br. 37. This, too, is an argument about the merits, not about standing, but it is worth pausing to consider its implications. If Wikimedia lacks standing to challenge the government's interception of its internal communications, presumably other organizations and businesses—libraries, banks, hospitals, schools—similarly lack standing to challenge the government's interception of *their* internal communications. Nor, on the government's view, would anyone else have standing to challenge the interception of those communications, because the patrons of those organizations do not (in the government's view) have standing to challenge the government's search and seizure of third-party business records containing their information. *See, e.g.*, *United States v. Graham*, 846 F. Supp. 2d 384, 388 (D. Md. 2012), *aff'd on other grounds*, No. 12-4659, 2015 WL 4637931, at *13–19 (4th Cir. Aug. 5, 2015). The government pretends to be arguing about who can challenge the surveillance at issue, but it is actually arguing that this surveillance should not be challengeable at all, by anyone.[20]

[20] Contrary to the government's suggestion, *see* Def. Br. 3, 21, where at least one plaintiff has demonstrated standing under Article III, a court "need not consider whether the other . . . plaintiffs have standing to maintain the suit." *Village of Arlington Heights v. Metro. Housing Dev. Corp.*, 429 U.S. 252, 264 & n.9 (1977).

B. In any event, the copying and review of Wikimedia's communications invades its protected privacy, possessory, and expressive interests.

The government casts Wikimedia's challenge as one that implicates only the rights of Wikimedia's community members and users, *see* Def. Br. 37, but Wikimedia has its own protected Fourth and First Amendment interests in the communications the NSA is intercepting. The government's standing argument is directly at odds with well-established precedents underscoring the Fourth and First Amendment interests of organizations, both non-profit and for-profit. *See, e.g.*, *Browning-Ferris Indus. of Vermont, Inc. v. Kelco Disposal, Inc*., 492 U.S. 257, 285 (1989) ("A corporation is . . . protected from unreasonable searches and seizures."); *cf. Marshall v. Barlow's, Inc*., 436 U.S. 307, 312 (1978) ("[I]t is untenable that the ban on warrantless searches was not intended to shield places of business as well as of residence."); *NAACP v. Button*, 371 U.S. 415, 428–29 (1963).

As set out above, Upstream surveillance implicates at least three categories of Wikimedia's communications: (1) its communications with community members who read and contribute to Wikimedia's websites; (2) its internal "log" communications; and (3) its communications by staff. The government challenges Wikimedia's *privacy* interest in the first two categories, Def. Br. 37, but not Wikimedia's protected possessory or expressive interests in those communications. The government ignores the third category of Wikimedia communications entirely.

1. Wikimedia has a possessory interest in its communications, which the government does not contest.

The Court need not reach the government's merits argument that Wikimedia lacks a privacy interest in its own communications, because Wikimedia has an undisputed *possessory* interest in the communications the government is intercepting. Am. Compl. ¶¶ 70, 103.

The government's copying of Wikimedia's external and internal communications interferes with a protected possessory interest—it deprives Wikimedia of the ability to control its information. *See United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (A seizure occurs when "there is some meaningful interference with an individual's possessory interests" in property.); *Carpenter v. United States*, 484 U.S. 19, 26 (1987) ("Confidential business information has long been recognized as property."). It is well-settled that the interception of communications while in transit is a seizure within the meaning of the Fourth Amendment. *See Ex parte Jackson*, 96 U.S. 727, 733 (1877); *Hearst v. Black*, 87 F.2d 68, 70–71 (D.C. Cir. 1936) (government's copying of telegrams in transit was a "dragnet seizure" that violated sender's possessory and privacy rights). This is true not only with respect to physical mail but with respect to digital communications as well, which may be "seized" through copying or recording. *See Katz v. United States*, 389 U.S. 347, 353 (1967) ("[E]lectronically listening to and recording the petitioner's words . . . constituted a 'search and seizure' within the meaning of the Fourth Amendment."). Indeed, the copying of information, in transit or otherwise, interferes with a possessory interest because it deprives its owner of the right to control that information. *See United States v. Jefferson*, 571 F. Supp. 2d 696, 702 (E.D. Va. 2008) (Ellis, J.); *LeClair v. Hart*, 800 F.2d 692, 696 & n.5 (7th Cir. 1986); *cf. Jacobsen*, 466 U.S. at 120–21 & n.18.

2. Wikimedia has a legitimate expectation of privacy in its communications.

Wikimedia also has a protected *privacy* interest in its real-time communications. *See Katz*, 389 U.S. at 353; *Browning-Ferris Indus. of Vermont, Inc.*, 492 U.S. at 285. Indeed, the government does not contest that Wikimedia has a privacy interest in the communications of its staff, Am. Compl. ¶¶ 102–04, nor could it. Organizations have a legitimate expectation of privacy in information they transmit, compile, or create, and a search of that information is an

injury that supports standing. *See, e.g.*, *City of Los Angeles v. Patel*, 135 S. Ct. 2443, 2448, 2452 (2015); 18 U.S.C. §§ 2510(6), 2520 (permitting corporations to bring claims under the Wiretap Act); 50 U.S.C. §§ 1801(i), 1810 (same under FISA).

Nonetheless, the government contends that Wikimedia lacks a privacy interest in its communications with community members and in its internal log communications because these two categories of communications contain only information about Wikimedia's users. Def. Br. 34–37. This argument is incorrect both factually and legally. As an initial matter, the government's description of these communications is a significant oversimplification. Even within these categories, Wikimedia's communications take many forms, and contain many different kinds of sensitive and private information—not only the IP addresses of those who read and contribute to the Projects. Am. Compl. ¶¶ 90–92 (describing the many types of data Wikimedia's HTTP/S communications reveal or contain). They include the "questions, comments, or complaints" that community members submit to Wikimedia about the performance and operation of its websites. *See id.* ¶¶ 90–91. They include internal, proprietary log entries, which Wikimedia compiles and transmits to help it monitor, study, and improve these websites. *Id.* ¶ 93. They include communications by user-community leaders who help administer the Wikimedia websites and deliberate on organizational decisions. *Id.* ¶¶ 92, 84. And they reveal private information about Wikimedia's operations, including details about its technical infrastructure, its data flows, and its member community writ large. *Id.* ¶ 99.

Wikimedia's communications also reveal who has contributed to its websites or visited them in search of information—and, just as importantly, exactly *what* information Wikimedia has exchanged with any individual user. *Id.* ¶¶ 98, 95–96. Except for those contributors who disclose their IP addresses, these exchanges are not public; they are private interactions between

Wikimedia and its community members. Only Wikimedia knows what any individual user is reading, and the privacy of these exchanges is essential to its mission—to fostering trust with community members so that they feel comfortable contributing to and visiting the site. *Id*. ¶ 98.

The government argues that the privacy interest in these communications belongs entirely to Wikimedia's users, Def. Br. 37, but the fact that an organization's records reflect the activities of its patrons, users, or customers does not mean that *only* those individuals have a privacy interest in the records. Indeed, the Supreme Court held recently in *Patel* that motel operators could bring a Fourth Amendment challenge to the search of their guest registries—logs that contain the name of each guest and details of his or her stay. 135 S. Ct. at 2447–48, 2452. Wikimedia's privacy interest in the communications at issue here is far stronger than that of the motel operators, who kept a relatively limited amount of information, and only for commercial purposes or because the law required them to. *See id.* at 2447.[21] The information at issue here goes to the core of Wikimedia's mission, and protecting it is critical to Wikimedia's ability to carry out activities protected by the First Amendment. Am. Compl. ¶ 98; *see Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (the Fourth Amendment should be applied with "scrupulous exactitude" when an organization's First Amendment activities are implicated).

The government also ignores the well-established principle that two parties communicating in real-time each have a privacy interest in their exchange. *See, e.g., United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 313 (1972); *see also* 50 U.S.C. § 1801(k). The existence of those interests does not depend on what they choose to communicate about, or

[21] *Patel* also makes clear that an organization's privacy interest does not depend on whether its records are created by a computer or by humans. 135 S. Ct. at 2448 (searches encompassing guest-registry logs created by automated check-in kiosks and maintained in electronic form). A rule to the contrary would have grave ramifications for the privacy interests of corporations, which of course compile and transmit many types of information exclusively using computers.

which way the information flows. Nor do these privacy interests disappear merely because the parties are exchanging information that is publicly available. The *fact* that the parties have chosen to communicate about certain information may be extraordinarily sensitive or revealing. *See Riley v. California*, 134 S. Ct. 2473, 2490 (2014) ("Internet search and browsing history . . . could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.").

Finally, the government objects that Wikimedia itself does not "learn the identity of the user" during the course of these communications, only his or her IP address. Def. Br. 35. But that is a red herring. The fact that users are identified by their IP address, rather than by name, does nothing to diminish the privacy interests in Wikimedia's communications. As the government well knows, it is generally easy to link a particular IP address with a particular person, especially in conjunction with other information—not least because IP addresses are often unique identifiers in much the same way that Social Security Numbers or phone numbers are.[22] Am. Compl. ¶ 94. Based on its communications, Wikimedia acquires a great deal of sensitive information about the everyday interests and concerns of its community members. *Id*. ¶¶ 94–96. That is precisely why the NSA points analysts to intercepted Wikimedia communications as a means of learning "nearly everything a typical user does on the Internet." *Id*. ¶ 107.

[22] The Lee Declaration suggests that the IP addresses associated with individual Wikimedia users are not personally identifying, Lee Decl. ¶¶ 20–22, but elsewhere the government has taken the opposite view. *See, e.g.*, Dep't of Homeland Security, *Privacy Impact Assessment for the Use of Google Analytics* 2, 3, 11 (June 9, 2011), http://1.usa.gov/1yCTj4A ("DHS shall not collect, maintain, or retrieve personally identifiable information (PII) including a visitor's Internet Protocol (IP) Address"); Dep't of the Interior, *Social Media Guidebook* 14, 19,30 (June 12, 2015), http://on.doi.gov/1EeWaKE ("DOI considers a full IP address as PII.").

3. Wikimedia has expressive and associational interests in its communications, which the government does not contest.

Wikimedia also has expressive and associational interests in its communications, which independently give it standing. Wikimedia functions, in many ways, as the world's largest library—one that supports a wide array of expressive activity. *Id*. ¶¶ 78–79. The best-known of Wikimedia's Projects is Wikipedia—a free internet encyclopedia that is one of the largest collections of shared knowledge in human history. *Id*. ¶ 79. The site also features several kinds of discussion spaces, and it encourages vigorous debate among its users. *Id.* In these activities, Wikimedia has a First Amendment right to distribute and receive information, to encourage the exchange of knowledge and opinions, and to associate privately with its community for all these purposes. *See Griswold v. Connecticut*, 381 U.S. 479, 482 (1965) ("The right of freedom of speech and press includes not only the right to utter or to print, but the right to distribute, the right to receive, the right to read."); *Shelton v. Tucker*, 364 U.S. 479, 485–86 (1960).

The communications the government is intercepting are one of the principal ways in which Wikimedia conducts its protected First Amendment activities. Am. Compl. ¶ 81. Its ability to carry out these activities depends on the confidentiality of its communications. *Id*. ¶¶ 89, 98, 108. Moreover, these communications are themselves records of Wikimedia's billions of day-to-day associations. *Id*. ¶¶ 87–93. They reveal the identities of those who associate with Wikimedia—as well as exactly what information each individual is exchanging with it, either by contributing to Wikimedia's store of knowledge or by reading what is already there. *Id*. ¶¶ 89, 95. Wikimedia has a First Amendment interest in these communications that is its own to assert, and that confers standing here. *See Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 64 n.6 (1963); *Thornburgh v. Abbott*, 490 U.S. 401, 408 (1989) (stating that publishers "have a legitimate First Amendment interest" in communicating with readers). Indeed, courts have found that

organizations engaged in First Amendment activities may bring claims challenging demands for their information, *even* where that information is sought from a third party. *See, e.g.*, *N.Y. Times Co. v. Gonzales*, 459 F.3d 160, 167–68 (2d Cir. 2006) (permitting newspaper to challenge subpoena to third-party provider for its phone records). Wikimedia certainly has standing here, where the NSA is intercepting its communications directly and surreptitiously.

C. Wikimedia also has third-party standing to assert the rights of its community members.

The government is also wrong when it argues that Wikimedia may not assert claims on behalf of its users. Wikimedia has standing to assert the rights of (1) U.S. persons abroad whose communications with Wikimedia are intercepted; and (2) the rights of individual users inside the United States, whose ability to exchange information with Wikimedia's foreign readers and editors has been impaired by Upstream surveillance. Am. Compl. ¶¶ 85, 110.

To begin with, third-party standing is a prudential question, not a constitutional one. *See, e.g.*, *Craig v. Boren*, 429 U.S. 190, 193 (1976). Thus, what the government calls "[t]he rule against third-party standing," Def. Br. 37, is far from "absolute." *Kowalski v. Turner*, 543 U.S. 125, 129 (2004). Indeed, in cases where the ability of individuals to speak, read, and write privately and anonymously is at stake—as it is here—the Supreme Court has been "quite forgiving" in applying its third-party standing test. *Kowalski*, 543 U.S. at 130; *see Sec'y of State v. Joseph H. Munson Co.*, 467 U.S. 947, 956 (1984) (explaining that "[s]ociety as a whole . . . would be the loser" if third parties could not assert First Amendment claims challenging statutes on behalf of others); *Cooksey v. Futrell*, 721 F.3d 226, 234 (4th Cir. 2013). Wikimedia has satisfied all three conditions for third-party standing: (1) an injury in fact; (2) a close relationship with the person who possesses the right; and (3) some obstacle to the possessor's ability to protect her own interests. *See Kowalski*, 543 U.S. at 130.

First, as explained above, Wikimedia itself has stated an injury in fact based on the interception of its communications. *See* Section II & III.A–B, *supra*.

Second, Wikimedia plainly enjoys an "active and close relationship" with many of the community members whose rights it seeks to protect. Am. Compl. ¶ 83 ("Wikimedia operates interdependently with its user community in pursuit of a shared set of free-knowledge values."); *see id.* ¶¶ 84, 101. Thus, Wikimedia users' "enjoyment of the[ir] right[s] is inextricably bound up" with Wikimedia's activity, and Wikimedia will be as effective a proponent of its users' rights as the users would be. *Singleton v. Wulff*, 428 U.S. 106, 114 (1976).

Finally, Wikimedia's users face clear obstacles to litigating their own rights in this context. As Plaintiffs explain, Wikimedia and its users depend on the ability to read, edit, and contribute to the Wikimedia Projects anonymously. Am. Compl. ¶¶ 98, 108. Courts have consistently determined that individuals' interest in preserving their anonymity is precisely the kind of "practical obstacle" to bringing suit that gives rise to third-party standing. *Enterline v. Pocono Med. Ctr.*, 751 F. Supp. 2d 782, 786 (M.D. Pa. 2008); *see also In re Drasin*, No. ELH-13-1140, 2013 WL 3866777, at *2 & n.3 (D. Md. July 24, 2013); *Amazon.com LLC v. Lay*, 758 F. Supp. 2d 1154 (W.D. Wash. 2010). Moreover, while the injuries to individual Wikimedia users are serious, an individual user will "possess[] little incentive to set in motion the arduous process needed to vindicate his own rights," *Powers v. Ohio*, 499 U.S. 400, 415 (1991); *see also Agostino v. Simpson*, No. 08 Civ. 5760, 2008 WL 4906140, at *6 (S.D.N.Y. Nov. 17, 2008) (finding lack of incentive to file suit sufficient to satisfy third prong).

IV. Plaintiffs have plausibly alleged standing for additional reasons.

A. Plaintiffs have plausibly alleged that they have been compelled to take burdensome and costly measures in response to Upstream surveillance.

Plaintiffs have plausibly alleged that they have been forced to take burdensome and costly measures as a result of Upstream surveillance—a separate injury in fact sufficient to confer standing. *See, e.g.*, *Monsanto*, 561 U.S. at 154–55; *Friends of the Earth v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 184–85 (2000); Am. Compl. ¶ 75. *Amnesty* is not to the contrary. There, the Supreme Court explicitly recognized that a plaintiff may establish standing by showing that he or she has had to incur costs to mitigate a substantial risk of harm. *See* 133 S. Ct. at 1150 n.5. The Court concluded, however, that because in that case the plaintiffs' preventive measures were taken in response to a "speculative threat," these measures did not confer standing. *See id.* at 1151. But there is nothing "speculative" about the threat of Upstream surveillance. *Id.* Rather, as explained in the Amended Complaint, Plaintiffs are taking burdensome and sometimes costly measures in response to the "virtual certainty" that their communications are being copied and reviewed in the course of Upstream surveillance. *See, e.g.*, Am. Compl. ¶¶ 67, 71, 109, 118, 128, 134, 144, 154, 164. Accordingly, Plaintiffs' preventive measures constitute a present injury sufficient to establish standing.

The necessity and reasonableness of these measures is clear. For example, NACDL member and criminal defense attorney Joshua Dratel has a client, Agron Hasbajrami, whose communications the government has officially acknowledged intercepting and retaining using FAA surveillance. Am. Compl. ¶ 121; Def. Br. 46 & n.31. Mr. Dratel had a second client, Sabirhan Hasanoff, whose prosecution also relied upon officially acknowledged FAA surveillance—in that case, involving the communications of another defendant in the same investigation. Am. Compl. ¶ 121; Def. Br. 47. What that means is that the government's

evidence in these criminal investigations was derived from FAA surveillance targeting one or more of the defendants' foreign *contacts*. As a result of this acknowledged surveillance, Mr. Dratel's own 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 in the course of investigating the government's allegations, contacting witnesses, and collecting research and evidence from sources abroad via the internet. Am. Compl. ¶ 127. In these circumstances, the rules of professional responsibility require Mr. Dratel to take reasonable precautions to maintain the confidentiality of his communications. *Id.* ¶ 128. Due in part to Upstream surveillance, in these representations and others, Mr. Dratel must employ burdensome electronic security measures to protect his communications, and in some instances he has had to travel abroad to gather information in person. *Id.* These precautions are not "simply the product of [his] fear of surveillance," nor are they voluntary responses to a speculative threat. *Amnesty*, 133 S. Ct. at 1152. They are the product of surveillance the government openly acknowledged only after *Amnesty* was decided,[23] including in cases where Mr. Dratel's client, his client's co-defendant, and key fact-witnesses overseas have been subject to FAA surveillance.

B. Plaintiffs have plausibly alleged that Upstream surveillance impairs their protected expressive activities.

As the Fourth Circuit has recognized, "First Amendment cases raise unique standing considerations that tilt dramatically toward a finding of standing." *Cooksey*, 721 F.3d at 235 (quoting *Lopez v. Candaele*, 630 F.3d 775, 781 (9th Cir. 2010)). "[W]hen there is a danger of

[23] *See* Letter from Sens. Ron Wyden, Mark Udall, and Martin Heinrich to Solicitor General Donald Verrilli (Nov. 20, 2013), http://bit.ly/1JcrJDU (criticizing the government's failure to notify criminal defendants of FAA surveillance despite the Solicitor General's representations to the Supreme Court that the government was providing such notice).

chilling free speech, the concern that constitutional adjudication be avoided whenever possible may be outweighed by society's interest in having the [state action] challenged." *Joseph H. Munson Co., Inc.*, 467 U.S. at 956. That Upstream surveillance impairs Plaintiffs' First Amendment activities supplies an independent basis for standing.

The Amended Complaint explains in detail how Plaintiffs' communications are subject to Upstream surveillance, and how this surveillance infringes upon their First Amendment rights. In the course of their work, Plaintiffs engage in a variety of First Amendment-protected activities, including journalism, advocacy, and the publication of educational material. *See* Am. Compl. ¶¶ 6–14. Upstream surveillance interferes with these protected activities in several ways. It makes it difficult, expensive, and sometimes impossible for NACDL members like Mr. Dratel to obtain information from individuals outside of the United States. In some instances, potential witnesses, clients, and other lawyers have limited the information that they share with Mr. Dratel, and some of them refuse to communicate with him electronically. *Id.* ¶ 129. More broadly, the NSA's surveillance activities compel Plaintiffs to self-censor their communications, and in some instances forgo electronic communications altogether. *See, e.g.*, *id*. ¶¶ 109, 128–29, 134, 139, 144, 149, 154, 159, 164. These concrete harms are sufficient to support standing. *See, e.g.*, *Cooksey*, 721 F.3d at 235 ("In First Amendment cases, the injury-in-fact element is commonly satisfied by a sufficient showing of 'self-censorship.'").[24]

[24] The government contends that certain of Plaintiffs' injuries—including their preventative measures and impaired expressive activities—are not "fairly traceable" to Upstream surveillance. *See* Def. Br. 16, 45, 48. This is not so. As an initial matter, Plaintiffs have plausibly alleged that their communications are subject to Upstream copying, review, and retention, and that this surveillance interferes with their rights—thus satisfying the traceability requirement.

Plaintiffs have further plausibly alleged that Upstream surveillance undermines their work, and that due in part to Upstream surveillance, they have taken various measures to protect their communications. *See, e.g.*, Am. Compl. ¶ 75. These harms are "readily attributable" to Upstream surveillance, and standing is not defeated by the existence of an intermediate link between the

C. Plaintiffs have plausibly alleged that the NSA is not only copying and reviewing their communications, but retaining them as well.

1. Plaintiffs have plausibly alleged a substantial likelihood that they communicate with individuals and organizations that are NSA targets.

As explained in the Amended Complaint, given the identities and locations of Plaintiffs' contacts, there is a substantial likelihood that the NSA has targeted at least some of those contacts—and therefore has copied, reviewed, and *retained* Plaintiffs' communications.[25] *See, e.g.*, Am. Compl. ¶¶ 79, 104 (Wikimedia's international contacts include millions of users, foreign telecommunication companies, and political and business leaders); *id.* ¶ 133 (HRW's international contacts include foreign government officials, humanitarian agencies, military officials, human rights defenders, victims of human rights abuses, media, and scholars); *id.* ¶ 148 (GFW's international contacts include foreign banks and foreign government agencies); *id.* ¶ 153 (The Nation's international contacts include foreign journalists in conflict zones and members of insurgency movements); *id.* ¶ 163 (WOLA communicates with foreign government officials—including at times presidents and ministers—as well as staff from multinational institutions, such as the United Nations); *see also* Section IV.A, *supra* (describing Mr. Dratel's foreign contacts). Because these are precisely the types of organizations and individuals that the government likely targets for foreign intelligence purposes—and because these Plaintiffs' communications with

---

challenged conduct and the injury. *Monsanto Co.*, 561 U.S. at 155; *Libertarian Party of Virginia v. Judd*, 718 F.3d 308, 316 (4th Cir. 2013) (a plaintiff meets the fairly traceable requirement if the defendant's conduct is "at least in part responsible for [plaintiff's injury] . . . . notwithstanding the presence of another proximate cause").

[25] To be clear, Plaintiffs need not separately establish that their communications are being retained in order to challenge Upstream surveillance and the procedures that govern it. *See, e.g.*, *Berger v. New York*, 388 U.S. 41, 58–59 (1967); *Nat'l. Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 663, 675–76 (1989). While the retention of their communications is a further, discrete injury, Am. Compl. ¶ 72, Plaintiffs have already shown that their communications are being copied and reviewed by the government, and this is sufficient to give them standing to challenge the lawfulness of Upstream surveillance.

these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information"—Plaintiffs have plausibly alleged a substantial likelihood that the NSA has targeted and retained their communications. *See* Am. Compl. ¶¶ 71, 104–05, 115–16, 125, 127, 133, 138, 143, 148, 153, 158, 163.[26]

2. Plaintiffs have plausibly alleged a substantial likelihood that they communicate *about* individuals and organizations that are NSA targets.

Plaintiffs have also plausibly alleged that there is a substantial likelihood that the NSA retains, reads, and disseminates their communications because they communicate *about* persons and organizations targeted for Upstream surveillance. *See id*. ¶¶ 104–06, 115, 126, 133, 138, 143, 148, 153, 158, 163. For instance, because one of the Wikimedia Projects, Wikipedia, is an exhaustive encyclopedic resource, it includes entries related to virtually every foreign organization or company the U.S. government might target for Upstream surveillance. *See id*. ¶ 106. Many of these descriptions contain references to website addresses and domain names associated with those potential targets. *Id.* Any time a user abroad visits or edits a page containing one of the government's targeted selectors, Wikimedia's communication with that user is retained, read, and disseminated by the NSA. *Id.* ¶ 105. Notably, website addresses or domain names associated with organizations on the U.S. State Department's Foreign Terrorist Organization list appear *over 700 times* on Wikimedia webpages—including within the encyclopedia entries describing organizations, like Uzbekistan's Islamic Jihad Union, whose communications the U.S. government has targeted using FAA surveillance. *Id.*

[26] The government's argument that Plaintiffs' allegations about their contacts are less specific than the summary judgment declarations in *Amnesty* is unavailing. *See* Def. Br. 42 n.30. Here, on a motion to dismiss, the Court "presume[s] that general allegations embrace those specific facts that are necessary to support the claim." *Defenders of Wildlife*, 504 U.S. at 561; *see Susan B. Anthony List*, 134 S. Ct. at 2342 ("[E]ach element must be supported . . . with the manner and degree of evidence required at the successive stages of the litigation."); Fed. R. Civ. P. 8(a)(1).

3. The government's retention of Plaintiffs' communications is all the more plausible in light of public disclosures.

Recent public disclosures further support the plausibility of Plaintiffs' allegations that the government has retained their communications. The government's argument to the contrary—that Plaintiffs know nothing about its "targeting practices," or the categories of information that it is authorized to retain—is simply incorrect. *See* Def. Br. 41–42. Since *Amnesty* was decided, the government has officially acknowledged key facts concerning its FAA targets, as well as extensive information about its retention and use of information collected via Upstream surveillance—including, of course, the fact that the government is retaining communications that are merely "about" its targets. Against the backdrop of these disclosures, Plaintiffs' allegations that there is a substantial likelihood the government is retaining, reading, and disseminating their communications are plainly plausible.

In the past two years, the public has learned that the scope of the government's targeting and retention is vast. In 2011 alone, Upstream surveillance resulted in the retention of 26.5 million communications. [*Redacted*], 2011 WL 10945618, at *26. The public has also learned that the total number of the government's FAA targets is enormous—92,707, individuals, groups, and organizations in one year alone—bolstering the already-substantial likelihood that Plaintiffs communicate both with and about those targets. *See* Am. Compl. ¶ 37.[27] In addition, the government has disclosed specific types of information it uses FAA surveillance to acquire, which includes communications concerning "counterterrorism"—a topic that some of Plaintiffs' international communications often touch upon. PCLOB Report 25 & n.71; *see, e.g.*, Am.

[27] The fact that the government has in some instances spoken generally about "FAA surveillance," does not undercut Plaintiffs' argument. *See* Def. Br. 18, 45. Given that the government's stated objective is to "reliably" and "comprehensively" acquire its targets' communications, *see* Am. Compl. ¶ 65, it is *implausible* that the NSA is not pursuing those communications using both Upstream surveillance and PRISM surveillance.

Compl. ¶¶ 73, 106, 116, 125–27. Finally, one of the NSA's own documents, published in the press and incorporated into the Amended Complaint, further corroborates the plausibility of Wikimedia's allegations that the government has targeted its international contacts for Upstream surveillance. This slide discusses the NSA's investigative interest in HTTP communications and is surrounded by the logos of major internet companies and websites, including Wikipedia. Am. Compl. ¶ 107.

These disclosures confirm the substantial likelihood that Plaintiffs' communications are retained in the course of Upstream surveillance, and render their allegations in the Amended Complaint all the more plausible. *See, e.g., id*. ¶¶ 73, 106, 127.[28]

CONCLUSION

For the reasons above, the government's motion to dismiss should be denied.

September 3, 2015

Respectfully submitted,

/s/
Deborah A. Jeon (Bar No. 06905)
David R. Rocah (Bar No. 27315)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838
jeon@aclu-md.org

/s/
Patrick Toomey (pro hac vice)
(*signed by Patrick Toomey with permission of Debbie A. Jeon*)
Jameel Jaffer (pro hac vice)
Alex Abdo (pro hac vice)
Ashley Gorski (pro hac vice)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500

[28] The government contends that NACDL has failed to identify a member who has alleged an injury in fact. *See* Def. Br. 42. To the contrary, NACDL has identified a member—Mr. Dratel—who is himself subject to each of the types of injury described above, including the copying, review, and retention of his communications. *See* Am. Compl. ¶¶ 119–29. Each of those allegations of injury is sufficient to establish that Mr. Dratel would have standing to bring suit, and accordingly, these allegations establish NACDL's standing. *See S. Walk at Broadlands Homeowner Ass'n v. Openband at Broadlands, LLC*, 713 F.3d 175, 184 (4th Cir. 2013).

Fax: (212) 549-2654
ptoomey@aclu.org

Charles S. Sims (pro hac vice)
David A. Munkittrick (pro hac vice)
John M. Browning (pro hac vice)
PROSKAUER ROSE LLP
Eleven Times Square
New York, NY 10036
Phone: (212) 969-3000
Fax: (212) 969-2900
csims@proskauer.com

Counsel for Plaintiffs