IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, *et al.*,	)	
Plaintiffs,	)	
	)	
v.	)	**Case No. 1:15-cv-662**
	)	
NATIONAL SECURITY AGENCY /	)	
CENTRAL SECURITY SERVICE, *et al.*,	)	
Defendants.	)	

MEMORANDUM OPINION

This is the latest in the recent series of constitutional challenges to the National Security Agency's ("NSA") data gathering efforts.[1] In this case, plaintiffs, nine organizations that communicate over the Internet, allege that the NSA's interception, collection, review, and storing of plaintiffs' Internet communications violates plaintiffs' rights under the First and Fourth Amendments and exceeds the NSA's authority under the Foreign Intelligence Surveillance Act ("FISA"). Typical of these challenges to the NSA's surveillance programs is defendants' threshold jurisdictional contention that plaintiffs lack Article III standing to assert their claims. This memorandum opinion addresses the standing issue.

---

[1] *See Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1144 (2013) (involving a facial challenge to Section 702 of the Foreign Intelligence Surveillance Act); *Obama v. Klayman*, Nos. 14-5004, 14-5005, 14-5016, 14-5017, 2015 WL 5058403 (D.C. Cir. Aug. 28, 2015) (involving a challenge to the NSA's bulk collection of telephone metadata produced by telephone companies); *Am. Civil Liberties Union v. Clapper*, 785 F.3d 787 (2d Cir. 2015) (involving a challenge to the NSA's bulk telephone metadata collection program); *Jewel v. Nat'l Sec. Agency*, No. C 08-04373, 2015 WL 545925 (N.D. Cal. Feb. 10, 2015), *appeal docketed*, No. 15-16133 (9th Cir. June 4, 2015) (involving a challenge to the NSA's interception of Internet communications).

I.[2]

The nine plaintiff organizations are as follows:

- Wikimedia Foundation ("Wikimedia") is a non-profit organization based in San Francisco, California, that maintains twelve Internet projects—including Wikipedia—that provide free content to users around the world.

- The National Association of Criminal Defense Lawyers ("NACDL") is a membership organization based in Washington, D.C., that focuses on criminal defense matters.

- Amnesty International USA, headquartered in New York City, is the largest division of Amnesty International, which focuses on human rights around the world.

- Human Rights Watch is a non-profit human rights organization based in New York City.

- PEN American Center is an association based in New York City that advocates on behalf of writers.

- Global Fund for Women is a non-profit grant-making foundation based in San Francisco, California, and New York City, that focuses on women's rights around the world.

- The Nation Magazine, published by The Nation Company, LLC, is based in New York City and reports on issues related to international affairs.

- The Rutherford Institute is a civil liberties organization based in Charlottesville, Virginia.

- The Washington Office on Latin America is a non-profit organization based in Washington, D.C., that focuses on social justice in the Americas.

The six defendants are the following government agencies and officers:

---

[2] The facts stated here are derived from the amended complaint and "documents incorporated into the complaint by reference," as is appropriate on a motion to dismiss. *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007). Plaintiffs' amended complaint incorporates, *inter alia*, the Privacy and Civil Liberties Oversight Board Report ("PCLOB Report") (July 2, 2014), the Office of the Director of National Intelligence Report ("ODNI Report") (April 22, 2015), the President's Review Group on Intelligence and Communications Technologies Report ("PRG Report") (Dec. 12, 2013), and [*Redacted*], 2011 WL 10945618 (FISA Ct. Oct. 3, 2011).

- The NSA is headquartered in Fort Mead, Maryland, and is the federal agency responsible for conducting the surveillance alleged in this case.
- The Department of Justice is a federal agency partly responsible for directing and coordinating the activities of the intelligence community, including the NSA.
- The Office of the Director of National Intelligence is a federal agency partly responsible for directing and coordinating the activities of the intelligence community, including the NSA.
- Adm. Michael S. Rogers is the Director of the NSA and the Chief of the Central Security Service.
- James R. Clapper is the Director of National Intelligence ("DNI").
- Loretta E. Lynch is the Attorney General of the United States.

A.

Before setting forth the facts alleged in the amended complaint ("AC"), it is useful to describe briefly the statutory context pertinent to the NSA's data gathering efforts. In 1978, in response to revelations of unlawful government surveillance directed at specific United States citizens and political organizations, Congress enacted FISA to regulate government electronic surveillance within the United States for foreign intelligence purposes. FISA provides a check against abuses by placing certain types of foreign-intelligence surveillance under the supervision of the Foreign Intelligence Surveillance Court ("FISC"), which reviews government applications for surveillance in certain foreign intelligence investigations. *See* 50 U.S.C. § 1803(a). As originally enacted, FISA required the government to obtain an individualized order from the FISC before conducting electronic surveillance in the United States. *See id.* § 1804(a). In this respect, the FISC could issue an order authorizing surveillance only if it found that 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 that "each of the facilities or places at which the electronic

surveillance [was] directed [was] being used, or [was] about to be used, by a foreign power or an agent of a foreign power." *Id.* § 1805(a)(2).

In 2008, thirty years after FISA's enactment, Congress passed the FISA Amendments Act, which established procedures and requirements for the authorization of surveillance targeting persons located outside the United States. *See* 50 U.S.C. §§ 1881a-1881g. Specifically, FISA Section 702, 50 U.S.C. § 1881a, "supplements pre-existing FISA authority by creating a new framework under which the [g]overnment may seek the FISC's authorization of certain foreign intelligence surveillance targeting ... non-U.S. persons located abroad," *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1144 (2013). Section 702 provides that the Attorney General and the Director of National Intelligence may jointly authorize, for up to one year, the "targeting of [non-U.S.] persons reasonably believed to be located outside the United States to acquire foreign intelligence information"[3] if the FISC approves "a written certification" submitted by the government that attests, *inter alia*, that (i) a significant purpose of the acquisition is to obtain foreign intelligence information and (ii) the acquisition will be conducted "in a manner consistent with the [F]ourth [A]mendment" and the targeting and minimization procedures required by statute. 50 U.S.C. § 1881a(b), (g). Specifically, before approving a certification, the FISC must find that the government's targeting procedures are reasonably designed:

> (i) to ensure that acquisition "is limited to targeting persons reasonably believed to be located outside the United States," *id.* § 1881a(i)(2)(B)(i);
>
> (ii) to prevent the intentional acquisition of wholly domestic communications, *id.* § 1881a(i)(2)(B)(ii);
>
> (iii) to "minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons

[3] Importantly, the statute expressly prohibits the intentional targeting of any person known at the time of acquisition to be in the United States or any U.S. person reasonably believed to be located outside the United States. 50 U.S.C. § 1881a(b).

> consistent with the need of the United States to obtain, produce, and disseminate foreign-intelligence information," *id.* § 1801(h)(1); *see id.* § 1881a(i)(2)(C); and
>
> (iv) to ensure that the procedures "are consistent with ... the [F]ourth [A]mendment," *id.* § 1881a(i)(3)(A).

In effect, an approval of government surveillance by the FISC means that the surveillance comports with the statutory requirements and the Constitution.

Additional details regarding the collection of communications under Section 702 have recently been disclosed in a number of public government reports and declassified FISC opinions. The government has disclosed, for example, that in 2011, Section 702 surveillance resulted in the retention of more than 250 million communications and that in 2014, the government targeted the communications of 92,707 individuals, groups, and organizations under a single FISC Order.[4] The total number of U.S. persons' communications that the government has intercepted or retained pursuant to Section 702 remains classified. The government has also disclosed that the NSA conducts two kinds of surveillance pursuant to Section 702. Under a surveillance program called "PRISM,"[5] U.S.-based Internet Service Providers furnish the NSA with electronic communications that contain information specified by the NSA. This case concerns the second method of surveillance, which is referred to as "Upstream surveillance."

B.

Plaintiffs challenge the NSA's use of Upstream surveillance, alleging that this mode of surveillance enables the government to collect communications as they transit the Internet

---

[4] *See* AC ¶ 37. The AC cites a redacted FISC Order and a government report for this information. *See* [*Redacted*], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011); ODNI Report, at 1, 2.

[5] "PRISM" is a government code name for a data-collection that is officially known as US-984XN. *See* PRISM/US-984XN Overview, April 2013, *available at* https://www. aclu.org/files/natsec/nsa/20130816/PRISM%20Overview%C20Powerpoint%20Slides.pdf (last visited Oct. 22, 2015).

"backbone," the network of high-capacity cables, switches, and routers that facilitates domestic and international Internet communication. With the assistance of telecommunications providers, Upstream surveillance enables the NSA to copy and review "text-based" communications—*i.e.*, those whose content includes searchable text, such as emails, search-engine queries, and webpages—for search terms called "selectors." Importantly, selectors cannot be key words or names of targeted individuals, but must instead be specific communications identifiers, such as email addresses, phone numbers, and IP addresses.

Plaintiffs allege that Upstream surveillance encompasses the following four processes, one or more of which is implemented by telecommunications providers at the NSA's direction:

> (i) Copying: Using surveillance devices installed at key access points along the Internet backbone, the NSA intercepts and copies text-based communications flowing across certain high-capacity cables and routers.
>
> (ii) Filtering: The NSA attempts to filter the copied data and discard wholly domestic communications, while preserving international communications. Because the NSA's filtering of domestic communications is imperfect, some domestic communications are not filtered out.
>
> (iii) Content Review: The NSA reviews the copied communications that are not filtered out for instances of tasked selectors.
>
> (iv) Retention and Use: The NSA retains all communications that contain selectors associated with its targets and other communications that were bundled in transit with the targeted communications; NSA analysts may read and query the retained communications and may share the results with the FBI.

See AC ¶¶ 40, 47-49.[6]

Plaintiffs emphasize two aspects of Upstream surveillance. First, surveillance under that program is not limited to communications sent or received by the NSA's targets, as the government has acknowledged that, as part of Upstream surveillance, the NSA also engages in what is called "about surveillance"—the searching of Internet communications that are *about* its

[6] Plaintiffs' description of Upstream surveillance is based on the PCLOB Report, at 32-41.

targets. AC ¶ 50. In other words, plaintiffs allege that the NSA intercepts substantial quantities of Internet traffic and examines those communications to determine whether they include references to the NSA's search terms. Second, Upstream surveillance implicates domestic communications because (i) the NSA's filters are imperfect, (ii) the NSA sometimes mistakes a domestic communication for an international one, and (iii) the NSA retains communications that happen to be bundled, while in transit, with communications that contain selectors.

All nine plaintiffs allege that the NSA uses Upstream surveillance to copy their Internet communications, filter the large body of collected communications in an attempt to remove wholly domestic communications, and then search the remaining communications with "selectors," looking for potentially terrorist-related foreign intelligence information. Plaintiffs further claim that these government actions invade their privacy—as well as the privacy of their staffs, Wikimedia's users, and NACDL's members—and infringe on plaintiffs' rights to control their communications and the information therein. Plaintiffs also allege that the NSA intercepts, copies, and reviews two other categories of communications specific to Wikimedia: (i) the over one trillion annual communications that plaintiffs claim occur when individuals around the globe view and edit Wikimedia websites and interact with one another on those sites; and (ii) Wikimedia's logs of online requests by such users to view its webpages. In addition to the claimed interception, copying, and selector review of their communications, plaintiffs allege that there is a "substantial likelihood" that plaintiffs' communications are retained, read, and disseminated by the NSA. *Id.* ¶ 71. This is so, plaintiffs allege, because plaintiffs, their members, and their employees communicate online with people whom the government is likely to target when conducting Upstream surveillance, and a significant amount of the information plaintiffs, their members, and their employees exchange with those persons constitutes "foreign

intelligence information" under FISA. *Id.* ¶ 74. Plaintiffs further allege that Upstream surveillance undermines their ability to carry out activities crucial to their missions (i) by forcing them to take burdensome measures to minimize the risk that the confidentiality of their sensitive information will be compromised and (ii) by reducing the likelihood that individuals will share sensitive information with them.

Plaintiffs claim that the alleged injuries result from the NSA's use of Upstream surveillance that violates the First and Fourth Amendments of the Constitution and exceeds the government's authority under Section 702.[7] By way of relief, plaintiffs seek a declaration that Upstream surveillance is unlawful, an injunction prohibiting the NSA from using Upstream surveillance to intercept plaintiffs' communications, and a purge from government databases of any of plaintiffs' communications acquired through Upstream surveillance.

Defendants have moved to dismiss plaintiffs' AC pursuant to Rule 12(b)(1), Fed. R. Civ. P., on the ground that plaintiffs lack Article III standing to contest the legality of the NSA's Upstream surveillance because plaintiffs have not alleged facts that plausibly establish an actual injury attributable to the NSA's Upstream surveillance.

II.

Article III limits the jurisdiction of federal courts to certain "Cases" and "Controversies." U.S. Const. art. III, § 2, cl. 2. As the Supreme Court has made clear, one "essential and unchanging part of the case-or-controversy requirement" is that a plaintiff must establish Article III standing to sue. *Lujan v. Defenders of Wildlife,* 504 U.S. 555, 560 (1992). A plaintiff establishes Article III standing by showing that he seeks relief from an injury that is "'concrete,

---

[7] Of course, the FISC opinion that relates to the data collection practices challenged here is unavailable because it is classified. It would be helpful and generally beneficial to the public for FISC opinions to be published by way of either declassification or redaction.

particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'" *Clapper*, 133 S. Ct. at 1147 (quoting *Monsanto Co. v. Geerston Seed Farms*, 561 U.S. 139, 149 (2010)). The alleged injury must be "real and immediate," not "conjectural or hypothetical," *City of Los Angeles v. Lyons*, 461 U.S. 95, 201 (1983). The Supreme Court has "repeatedly reiterated that '[a] threatened injury must be *certainly impending* to constitute injury in fact,' and that '[a]llegations of *possible* future injury' are not sufficient." *Clapper*, 133 S. Ct. at 1147 (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)) (emphases in original). Importantly, the standing inquiry is "especially rigorous when reaching the merits of the dispute would force [a court] to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional," particularly "in the fields of intelligence gathering and foreign affairs." *Clapper*, 133 S. Ct. at 1147.

Because standing is a threshold jurisdictional requirement, it may be attacked at any time, including at the outset of a case pursuant to Rule 12(b)(1), Fed. R. Civ. P. As the Fourth Circuit has made clear, where, as here, "standing is challenged on the pleadings, [a court must] accept as true all material allegations of the complaint and construe the complaint in favor of the complaining party." *David v. Alphin*, 704 F.3d 327, 333 (4th Cir. 2013) (citing *Pennell v. City of San Jose*, 485 U.S. 1, 7 (1988)). But a court should not "take account of allegations in the complaint labeled as fact but that constitute nothing more than 'legal conclusions' or 'naked assertions.'" *Id.* (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)). A complaint must contain "sufficient factual matter, accepted as true, to 'state a claim that is plausible on its face.'" *Ashcroft*, 556 U.S. at 678 (2009) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). Standing is adequately alleged only if the "well-pleaded allegations" allow for a

"reasonable inference," rather than a "sheer possibility," that the plaintiff has standing, *Iqbal*, 556 U.S. at 678-79; *David*, 704 F.3d at 333.[8]

III.

Clapper v. Amnesty International is the Supreme Court's most recent pronouncement on standing with respect to litigants challenging the NSA's data gathering efforts, and therefore is the leading case in this series. In *Clapper*, the plaintiffs argued that they had standing to bring a facial challenge to Section 702 because there was an "objectively reasonable likelihood" that plaintiffs' communications "[would] be intercepted" in the future. 133 S. Ct. at 1147. The Supreme Court rejected this "novel view of standing" because plaintiffs' "speculative chain of possibilities [did] not establish that injury based on future surveillance [was] certainly impending or [was] fairly traceable to [Section 702 surveillance]." *Id.* at 1146, 1150. Of course, if the alleged facts and arguments in this case are essentially identical to those in *Clapper,* then *Clapper* must control the result reached here. On the other hand, if plaintiffs in this case present facts and arguments that are different from those asserted in *Clapper*, then those facts and arguments must be carefully considered to determine whether they compel a result different from *Clapper*.

---

[8] As the parties correctly note, a jurisdictional motion to dismiss may be brought as a facial or factual challenge. *Adams v. Bain*, 697 F.2d 1213, 1219 (4th Cir. 1982). On a factual challenge, "a trial court may 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." *Id.*; *see also Kerns v. United States*, 585 F.3d 187, 193 (4th Cir. 2009). When appropriate, a court may also 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) (granting jurisdictional discovery "to allow consideration of [a] pivotal issue on a more complete record"). Here, defendants have brought a facial challenge, but have also submitted declarations and accompanying exhibits not incorporated by reference in the complaint. As plaintiffs correctly note, this additional evidence is properly considered only if the motion to dismiss is decided on a factual—rather than facial—basis. Because the dispute can be resolved on the face of the complaint, the additional declarations and exhibits are not considered.

In the course of oral argument, plaintiffs' counsel was asked to identify the facts and arguments in this case that are different from those asserted in *Clapper*.[9] Plaintiffs' counsel identified four differences:

> (i) the legal standard in this case is different from the legal standard that controlled in *Clapper* because the standing challenge here arises on a motion to dismiss rather than, as in *Clapper*, on a motion for summary judgment.
>
> (ii) far more is known about Section 702 surveillance, including Upstream surveillance, than was known at the time of *Clapper*;
>
> (iii) the Upstream surveillance at issue here is fundamentally different from the surveillance at issue in *Clapper*; and
>
> (iv) plaintiffs here are different from the *Clapper* plaintiffs in important respects concerning their Internet communications.[10]

Clearly there are differences between the facts and arguments raised in this case and those raised in *Clapper*, but the question is not simply whether there are differences, but whether those differences compel the same or a different result from the result reached in *Clapper*.

Before addressing plaintiffs' arguments, it is important to describe *Clapper* in more detail. Plaintiffs in *Clapper* brought a facial challenge to Section 702, seeking a declaration that Section 702 was unconstitutional and an injunction against the surveillance authorized by that provision. 133 S. Ct. at 1142-46. The Supreme Court's opinion began its consideration of the standing issue by reviewing what was known and alleged concerning the NSA's surveillance practices under Section 702. Specifically, the Supreme Court explained that Section 702 surveillance "[was] subject to statutory conditions, judicial authorization, congressional supervision, and compliance with the Fourth Amendment," emphasizing that the government must obtain the FISC's "approval of 'targeting' procedures, 'minimization' procedures, and a

---

[9] Mot. to Dismiss Hr'g Tr. 19:13-16 (Sept. 25, 2015).

[10] *Id.* at 20:4-6, 21:12-14, 23:4-7, 27:17-21.

governmental certification regarding proposed surveillance." *Id.* at 1144, 1145 (quoting 50 U.S.C. § 1881a(a), (c)(1), (i)(2), (i)(3)). As the Supreme Court's opinion noted, "the [FISC's] role includes determining whether the [g]overnment's certification contains the required elements"[11] and whether the government's targeting procedures are "'reasonably designed' (1) to 'ensure that an acquisition ... is limited to targeting persons reasonably believed to be located outside the United States' and (2) to 'prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known ... to be located in the United States." *Id.* at 1135 (quoting 50 U.S.C. § 1881a(i)(2)(B)).

The Supreme Court explained that in attempting to establish standing, the *Clapper* plaintiffs did not provide "any evidence that their communications ha[d] been monitored under" any program authorized by Section 702. *Id.* at 1148. Instead, plaintiffs argued that they had standing because there was an "objectively reasonable likelihood" that plaintiffs' communications "[would] be intercepted" in the future. *Id.* at 1147. The Supreme Court's opinion characterized plaintiffs' argument as a "speculative chain of possibilities," *id.* at 1150.[12]

---

[11] As the *Clapper* majority further explained, the "[g]overnment's certification must attest" (1) that the procedures in place "'have been approved, have been submitted for approval, or will be submitted with the certification for approval by the [FISC]'" and "'are reasonably designed' to ensure that an acquisition is 'limited to targeting persons reasonably believed to be located outside' the United States;" (2) that the "minimization procedures adequately restrict the acquisition, retention, and dissemination of nonpublic information about unconsenting U.S. persons, as appropriate;" (3) that "guidelines have been adopted to ensure compliance with targeting limits and the Fourth Amendment;" and (4) that "the procedures and guidelines referred to above comport with the Fourth Amendment." *Id.* at 1145 (quoting 50 U.S.C. § 1881a(g)(2)).

[12] The speculative chain consisted of five contingencies: (i) that the "[g]overnment [would] decide to target the communications of non-U.S. persons with whom [plaintiffs] communicate;" (ii) that in targeting those communications, "the [g]overnment [would] choose to invoke its authority under [Section 702] rather than utilizing another method of surveillance;" (iii) that "the Article III judges who serve on the [FISC would] conclude that the Government's proposed surveillance procedures satisfy [Section 702's] many safeguards and are consistent with the Fourth Amendment;" (iv) that upon such a finding by the FISC, "the Government [would]

The *Clapper* plaintiffs also argued that "they should be held to have standing because otherwise the constitutionality of [Section 702 surveillance] could not be challenged" and would be "insulate[d]" from "meaningful judicial review." The Supreme Court rejected that argument as "both legally and factually incorrect." *Id.* at 1154. The Supreme Court explained that Section 702 surveillance orders are not in fact insulated from judicial review because (i) the FISC reviews targeting and minimization procedures of Section 702 surveillance, (ii) criminal defendants prosecuted on the basis of information derived from Section 702 surveillance are given notice of that surveillance and can challenge its validity, and (iii) electronic communications service providers directed to assist the government in surveillance may challenge the directive before the FISC. *Id.* Even if these other avenues for judicial review were not available, the Supreme Court made clear that "'[t]he assumption that if [plaintiffs] have no standing to sue, no one would have standing, is not a reason to find standing.'" *Id.* (quoting *Valley Forge Christian College v. Americans United for Separation of Church and State, Inc.*, 454 U.S. 464, 489 (1982)).

In holding that plaintiffs' alleged injury was speculative, the *Clapper* majority rejected the approach advocated by the dissenting Justices. The dissent relied on "commonsense inferences" to find a "very high likelihood" that the government would "intercept at least some of" plaintiffs' communications. *Id.* at 1157 (Breyer, J., dissenting). Specifically, the dissent concluded that (i) the plaintiffs regularly engaged in the type of electronic communications that the government had "the capacity" to collect, (ii) the government was "strong[ly] motiv[ated]" to intercept for counter-terrorism purposes the type of communications in which plaintiffs engaged, and (iii) the government had in fact intercepted the same type of communications on thousands

---

succeed in intercepting the communications of plaintiffs' contacts;" and (v) that "[plaintiffs would] be parties to the particular communications that the Government intercept[ed]." *Id.* at 1148.

of occasions in the past. *Id.* at 1157-59 (Breyer, J. dissenting). The dissent also noted that the government had not "describe[d] any system for avoiding the interception of an electronic communication" to which plaintiffs were a party. *Id.* at 1159. Without evidence that a system was in place to prevent government interception of plaintiffs' communications,[13] the dissent reasoned that "we need only assume that the [g]overnment is doing its job (to find out about, and combat, terrorism) in order to conclude that there is a high probability that the [g]overnment will intercept at least some electronic communication to which at least some of the plaintiffs are parties." *Id.*

In essence, the Supreme Court held that the *Clapper* plaintiffs' chain of probabilities and inferences—based on the government's capacity and motivation to intercept communications similar to the *Clapper* plaintiffs' communications—was speculative, and therefore did not establish standing. The dissent, on the other hand, was convinced that such inferences and probabilities were sufficient to establish standing. At issue here is whether the four differences plaintiffs have identified compel the same or a different result from the result reached in *Clapper*. Each of plaintiffs' arguments with respect to those differences is separately addressed.

A.

Plaintiffs first argue that *Clapper* does not control here on the ground that the legal standard in this case is different from the legal standard applicable in *Clapper* because the standing challenge in the present case arises on a motion to dismiss rather than, as in *Clapper*, on a motion for summary judgment. To the extent this argument refers to the difference between reliance on factual allegations and reliance on a factual record, plaintiffs are undoubtedly correct.

---

[13] The majority noted that "[t]he dissent attempt[ed] to downplay the safeguards," as it "[did] not directly acknowledge that [Section 702] surveillance must comport with the Fourth Amendment … and that the [FISC] must assess whether targeting and minimization procedures are consistent with the Fourth Amendment." *Id.* at 1145 n.3.

The Supreme Court has made clear that, because the elements of standing are "an indispensable part of the plaintiff's case, each element must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e.*, with the manner and degree of evidence required at the successive stages in litigation." *Lujan*, 504 U.S. at 561. At the summary judgment stage, a plaintiff cannot rest simply on allegations, but must "'set forth' by affidavit or other evidence 'specific facts;'" at the motion to dismiss stage, however, "allegations of injury resulting from defendant's conduct may suffice." *Id.* at 561 (quoting Rule 56(2), Fed. R. Civ. P.).

But to say the evidentiary basis is different is not to say that the standing requirements change at each successive stage. They do not. The means by which a plaintiff establishes standing—by allegation or by record evidence—changes, but the three elements of standing—actual injury, causation, and redressability—remain constant and applicable at all stages of the case. This is so because standing is a jurisdictional requirement that "is an essential and unchanging part of the case-or-controversy requirement of Article III." *Id.* at 560. Indeed, the three elements of standing are the "irreducible constitutional minimum" that "set[] apart the 'Cases' and 'Controversies' that are of the sort referred to in Article III—'serv[ing] to identify those disputes which are appropriately resolved through the judicial process." *Id.* (quoting U.S. Const. art. III, § 2, cl. 2; *Whitmore*, 495 U.S. at 155).

Thus, to withstand defendants' standing challenge on a motion to dismiss, plaintiffs must allege facts that plausibly establish (i) that there is an "injury in fact—an invasion of a legally protected interest which is concrete and particularized and actual or imminent, not conjectural or hypothetical;" (ii) that the injury is "fairly trace[able] to the challenged action of the defendant;" and (iii) that it is "likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Id.* at 560-61. A court must, of course, "accept as true all material

allegations of the complaint and construe the complaint in favor of the complaining party," but a court should not "take account of allegations in the complaint labeled as fact but that constitute nothing more than 'legal conclusions' or 'naked assertions.'" *David*, 704 F.3d at 333 (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)). In short, a complaint alleges facts that plausibly establish standing only if the "well-pleaded allegations" allow for a "reasonable inference," rather than a "sheer possibility," that the plaintiff has satisfied each of the three elements of standing. *Iqbal*, 556 U.S. at 678-79; *David*, 704 F.3d at 333.

In sum, the standing requirement—the "irreducible constitutional minimum"—applies here just the same as it applied in *Clapper*. *Lujan*, 504 U.S. at 560. Moreover, the result in *Clapper*—that standing cannot be established on the basis of a "speculative chain of possibilities"—also applies here. 133 S. Ct. at 1150. Whether speculation is based on allegations in a complaint or facts in a record has no bearing on the outcome, as in neither context may standing be established on a "speculative chain of possibilities." *Id.*

B.

Plaintiffs next argue that *Clapper* does not control this case because more is now known about Section 702 surveillance, including Upstream surveillance, than was known at the time of *Clapper*. Plaintiffs cite in their AC several publicly disclosed documents in support of the allegation that the NSA uses Upstream surveillance to intercept substantially all international text-based Internet communications, including plaintiffs' communications.[14] Specifically, plaintiffs describe the technical features that enable the NSA to use Upstream surveillance to copy and review all or substantially all international text-based Internet communications, and the "strategic imperatives" that compel it to do so. Pls. Opp. Br. at 17. The AC alleges that:

---

[14] The AC cites, among other things, the PCLOB Report, the ODNI Report, the PRG Report, and [Redacted] , 2011 WL 10945618 (FISA Ct. Oct. 3, 2011).

(i) the Internet backbone funnels most communications entering or leaving the United States through 49 international chokepoints, AC ¶ 46;

(ii) the NSA has installed surveillance equipment at seven of those chokepoints, and the NSA has a strong incentive to intercept communications at more chokepoints in order to obtain the communications it seeks, *id.* ¶¶ 65-66, 68;

(iii) the installed surveillance equipment is capable of "examin[ing] the contents of all transmissions passing through," *id.* ¶ 62 (quoting PCLOB Report, at 122);

(iv) in order to identify the targeted communications, the NSA must copy and review the contents of an enormous quantity of transiting communications, *id.* ¶¶ 50, 51, 62; and

(v) because the NSA cannot know in advance which Internet "packets"[15] relate to its targets, the NSA, in order to be successful, must copy and reassemble all the packets associated with international text-based communications that transit the circuits it is monitoring, *id.* ¶¶ 42, 63-64.

Plaintiffs' series of allegations does not establish Article III standing because those allegations depend on suppositions and speculation, with no basis in fact, about how the NSA implements Upstream surveillance. Specifically, plaintiffs assume that the fact that Upstream surveillance equipment has been installed at some of the Internet backbone chokepoints implies that the NSA is intercepting all communications passing through those chokepoints. That may or may not be so; plaintiffs merely speculate that it is so. Even if the NSA's surveillance equipment is capable of "examin[ing] the contents of all transmissions passing through collection devices," as plaintiffs allege, *id.* ¶ 62, it does not follow that the NSA is, in fact, using the surveillance equipment to its full potential. As with any piece of technology, technical capability is not tantamount to usage levels. For example, a car capable of speeds exceeding 200 mph is not necessarily driven at such speeds; more information is needed to conclude that the top speed is reached. And there may indeed be circumstances that suggest a limited level of use—*e.g.*, a

[15] All Internet communications are broken into "packets"—discrete chunks of information—that traverse a variety of physical circuits. AC ¶ 42. Once the packets that make up a particular communication reach their final destination, they are reassembled. *Id.*

speed limit of 70 mph. The same is true here. Plaintiffs provide no factual basis to support the allegation that the NSA is using its surveillance equipment at full throttle,[16] and the fact that all NSA surveillance practices must survive FISC review—*i.e.*, must comport with the Fourth Amendment—suggests that the NSA is not using its surveillance equipment to its full potential. In addition, plaintiffs assume that the NSA must be intercepting communications at all 49 chokepoints because the NSA has a strong incentive to do so. But apart from plaintiffs' suppositions and speculation concerning the government's incentive and decision to act in accordance with that incentive, plaintiffs provide no factual basis that the NSA is actually intercepting communications at all chokepoints.

Plaintiffs cannot provide a sufficient factual basis for their allegations because the scope and scale of Upstream surveillance remain classified, leaving plaintiffs to prop their allegation of actual injury on suppositions and speculation about how Upstream surveillance *must* operate in order to achieve the government's "stated goals." AC ¶ 64. Indeed, plaintiffs cite the government's so-called "stated goals" in nearly every facet of their argument, specifically in support of their allegations regarding: (i) the volume of communications collected by Upstream surveillance, Pls. Opp. at 22, 28; (ii) the geographic distribution of the sites at which Upstream collection occurs, *id.* at 25; and (iii) the scope of Upstream surveillance at any site where it occurs, *id.* at 23, 30. It is, of course, a "possibility" that the NSA conducts Upstream surveillance

---

[16] Plaintiffs' AC cites a newspaper article that claimed "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." 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. But the article's claim is speculative, as it is based on a publicly disclosed document that says the NSA "seeks to acquire communications about the target that are not to or from the target" but does not indicate that the NSA is *actually* acquiring vast amounts of internet communications. *Id.* Indeed, the PCLOB Report—another document on which plaintiffs rely—refers to the article's claim as "represent[ing] a misunderstanding of a more complex reality." PCLOB Report, at 119.

in the manner plaintiffs allege, but this "bare assertion[]" is unaccompanied by "factual matter" that raises it "above a speculative level," and hence does not establish standing. *Iqbal*, 556 U.S. at 681.

In sum, plaintiffs are correct that more is known about the nature and capabilities of NSA surveillance than was known at the time of *Clapper*, but no more is known about whether Upstream surveillance *actually* intercepts all or substantially all international text-based Internet communications, including plaintiffs' communications. Thus, although plaintiffs' speculative chain is shorter than was the speculative chain in *Clapper*, it is a chain of speculation nonetheless. And *Clapper* makes clear that it is not the length of the chain but the fact of speculation that is fatal. Indeed, plaintiffs' reliance on the government's capacity and motivation to collect substantially all international text-based Internet communications is precisely the sort of speculative reasoning foreclosed by *Clapper*.[17] An alleged injury that is "speculative" does not establish Article III standing, especially the standing of litigants who seek to challenge the constitutionality of government action in the field of foreign intelligence. *Clapper*, 133 S. Ct. 1147-50.[18]

---

[17] As described above, the Supreme Court in *Clapper* rejected the argument that standing could be based on a "very strong likelihood" that the NSA would "intercept at least some of plaintiffs' communications" based on speculation about the government's "motivat[ion]" to exercise its "capacity" for such interception. 133 S. Ct. at 1159 (Breyer, J., dissenting). The same line of speculative reasoning was recently rejected by the D.C. Circuit in a case involving NSA surveillance. *Klayman*, 2015 WL 5058403, at *7 (Williams, J.) (holding that the plaintiffs' standing to challenge NSA bulk collection of telephone records could not be grounded in "their assertion that NSA's collection must be comprehensive in order for the program to be most effective").

[18] *See also Klayman*, 2015 WL 5058403, at *6 (Williams, J.) (noting that, although plaintiff may plausibly show why "the effectiveness of the program [would] expand with its coverage," such a showing does not make plaintiffs' claims of actual injury any less speculative).

C.

Plaintiffs further allege that *Clapper* does not control here because newly disclosed information reveals that Upstream surveillance is fundamentally different from the surveillance at issue in *Clapper*. Specifically, Upstream surveillance involves the use of "about surveillance," which the NSA allegedly uses to review every portion of everyone's communications—a broader mode of surveillance than the targeted surveillance of particular individuals' communications that was at issue in *Clapper*. Plaintiffs contend that "about surveillance" 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." Pls. Br. at 10. This analogy is inapt; contrary to plaintiffs' contention, the publicly disclosed documents on which plaintiffs rely do not state facts that plausibly support the proposition that "about surveillance" involves examining *every* portion of *every* copied communication. According to the PCLOB Report cited by plaintiffs,

> [T]he NSA's 'upstream collection' ... may require access to a larger body of international communications than those that contain a tasked selector[,] ... [but] the government has no ability to examine or otherwise make use of this larger body of communications, except to promptly determine whether any of them contain a tasked selector.

PCLOB Report, at 111 n.476. Indeed, "[o]nly those communications ... that contain a tasked selector go into government databases." *Id.* Thus, plaintiff's contention that "about surveillance" is like the hypothetical government agent reading every piece of mail misses the mark. Unlike the hypothetical government agent reading every word of every communication and retaining the information, "about surveillance" is targeted insofar as it makes use of only those communications that contain information matching the tasked selectors.

Even if plaintiffs' description of "about surveillance" were correct, it would not change the result reached here. Plaintiffs' claim of actual injury resulting from "about surveillance" rests

on plaintiffs' allegation that the NSA uses Upstream surveillance to intercept substantially all international text-based Internet communications. And as already discussed, that allegation is a "bare assertion[]" unaccompanied by "factual matter" that raises it "above a speculative level." *See Iqbal*, 556 U.S. at 681; *see also Clapper*, 133 S. Ct. at 1150. Details about the tools of Upstream surveillance reveal how Upstream surveillance functions when the NSA engages in that mode of surveillance, but those details do not cure the speculative foundation on which plaintiffs' claim of actual injury is based—that the NSA is *in fact* using Upstream surveillance to intercept substantially all text-based international Internet communications, including plaintiffs' communications.

D.

Plaintiffs next argue that *Clapper* does not control here because plaintiffs are different from the *Clapper* plaintiffs in important respects concerning their Internet communications. Although six of the nine plaintiffs in this case were plaintiffs in *Clapper*, plaintiffs identify two differences related to the new parties: (i) two clients of an NACDL attorney have received notice that they are targets of Section 702 surveillance and (ii) Wikimedia engages in over one trillion communications each year that are distributed around the globe.

1. NACDL Attorney Dratel

With respect to the first difference, plaintiffs argue that they adequately allege an actual injury because the government acknowledged that NACDL attorney Joshua Dratel's client, Agron Hasbajrami, was subject to Section 702 surveillance and another Dratel client, Sabirhan Hasanoff, was prosecuted on the basis of officially acknowledged Section 702 surveillance.[19]

---

[19] *See* Letter re Supplemental Notification, *United States v. Hasbajrami*, 1:11-cr-00623, ECF No. 65 (E.D. N.Y. Feb. 24, 2014); *See* Mem. Of Law, *Hasanoff v. United States*, 10 Cr. 162 (S.D.N.Y. Feb. 11, 2015), ECF No. 208, at 10-11.

Plaintiffs allege that as a result of this government acknowledged surveillance, Dratel's own international Internet communications were *likely* intercepted and retained because he *almost certainly* communicated with or about the targeted foreign individuals in the course of representing his clients. As plaintiffs note, Dratel's scenario is similar to a hypothetical mentioned in *Clapper*, in which the government "monitors [a] target's conversations with his or her attorney." 133 S. Ct. at 1154. The Supreme Court in *Clapper* described such a scenario as likely "hav[ing] a stronger evidentiary basis for establishing standing" than the *Clapper* plaintiffs had. *Id.* at 1154.

Here, however, the facts alleged differ from the *Clapper* hypothetical in important respects. The Supreme Court in *Clapper* was describing a situation in which there was some basis for an allegation that the government had "monitor[ed a] target's conversations with his or her attorney" using the type of surveillance at issue in the case, not a situation where an attorney lacks "concrete evidence to substantiate [his] fears." *Id.* Plaintiffs in this case, by contrast, do not allege facts that plausibly establish that the information gathered from the two instances of Section 702 surveillance was the product of Upstream surveillance. In neither of Dratel's cases did the government indicate whether the information at issue was derived from PRISM or Upstream surveillance, and no factual allegations in the AC plausibly establish that Upstream surveillance—rather than PRISM—was used to collect the information. Moreover, given what is known about the two surveillance programs, it appears substantially more likely that PRISM collection was used in these cases because, according to a 2011 FISC Order, the "vast majority" of collected communications are obtained via PRISM, not Upstream surveillance. [*Redacted*], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011) (finding that "upstream collection

constitute[d] only approximately 9% of the total Internet communications [then] acquired by [the] NSA under Section 702").

2. Wikimedia

Plaintiffs next allege that Wikimedia has standing because it is "virtually certain" that Upstream surveillance has intercepted at least some of Wikimedia's communications given the volume and geographic distribution of those communications. Specifically, Wikimedia allegedly engages in more than one trillion international text-based Internet communications each year and exchanges information with individuals in nearly every country on earth.

At the outset, an important implication of plaintiffs' allegation regarding Wikimedia's Internet communications must be noted. Plaintiffs have not alleged that any of the other eight plaintiffs (besides Wikimedia) engage in a substantial number of text-based international Internet communications. Indeed, plaintiffs simultaneously allege that (i) all nine plaintiffs "collectively engage in more than a trillion sensitive international [I]nternet communications each year," AC ¶ 58; and (ii) "Wikimedia engages in more than one trillion international communications each year," *id.* at ¶ 88. The AC does not quantify the other eight plaintiffs' communications. Thus, insofar as plaintiffs seek to establish standing on the basis of probabilities grounded in the volume of communications, plaintiffs' effort is limited to Wikimedia, as the AC says nothing about the volume of the other plaintiffs' communications.

With respect to Wikimedia, plaintiffs contend that Wikimedia's communications traverse all of the chokepoints at which the NSA conducts Upstream surveillance, however many that may be.[20] Plaintiffs argue that, because Upstream surveillance could achieve the government's

---

[20] The government has acknowledged using Upstream surveillance to monitor communications on more than one "international Internet link" or "circuit" on the Internet backbone. *Id.* at *15;

stated goals *only if* Upstream surveillance involved the copying and review of a large percentage of internatinoal text-based Internet traffic at each chokepoint that is monitored, it is virtually certain that the government has copied and reviewed at least one of Wikimedia's communications. Specifically, plaintiffs assume a 0.00000001% chance that any particular text-based Internet communication will be copied and reviewed by the NSA to conclude that the odds of the government copying and reviewing at least one of plaintiffs' over one trillion communications in a one-year period would be greater than 99.9999999999%. AC ¶ 58. Given the large volume of Wikimedia's communications with individuals all over the world, plaintiffs claim that some of Wikimedia's communications *almost certainly* traverse every major Internet circuit connecting the United States with the rest of the world. *Id.* ¶ 61.

Plaintiffs' argument is unpersuasive, as the statistical analysis on which the argument rests is incomplete and riddled with assumptions. For one thing, plaintiffs insist that Wikimedia's over one trillion annual Internet communications is significant in volume.[21] But plaintiffs provide no context for assessing the significance of this figure. One trillion is plainly a large number, but size is always relative. For example, one trillion dollars are of enormous value, whereas one trillion grains of sand are but a small patch of beach. Here, the relevant universe for comparison purposes is the total number of annual Internet communications, a figure that plaintiffs do not provide—nor even attempt to estimate—in the AC. Without defining the universe of the total number of Internet communications, it is impossible to determine whether

---

PCLOB Report 36–37. Plaintiffs, citing a publicly disclosed NSA document, allege that the NSA has installed Upstream surveillance equipment at seven of the 49 chokepoints. *See* AC ¶ 68.

[21] AC ¶ 58 ("[T]he sheer volume of [p]laintiffs' communications makes it virtually certain that the NSA has intercepted, copied, and reviewed at least some of those communications.").

Wikimedia's alleged one trillion annual Internet communications is significant or just a drop in the bucket of all annual Internet communications.

Moreover, plaintiffs conclude that there is a greater than 99.9999999999% chance that the NSA has intercepted at least one of their over one trillion communications on the basis of an arbitrary assumption, namely that there is a 0.00000001% chance that the NSA will intercept any particular Internet communication. AC ¶ 58. Plaintiffs provide no basis for the 0.00000001% figure, nor do they explain why the figure is presented as a conservative assumption.[22] Plaintiffs seem to presume a string of zeros buys legitimacy. It does not. Indeed, a closer looks reveals that the number of zeros chosen by plaintiffs leads conveniently to plaintiff's desired result. If three more zeros are added to plaintiffs' figure (0.00000000001%), the odds that at least one of Wikimedia's one trillion annual communications is intercepted drops to approximately 10%. If four more zeros are added (0.000000000001%), the odds that at least one of Wikimedia's communications is intercepted drops to 1%. In short, plaintiffs' assumption appears to be the product of reverse engineering; plaintiffs first defined the conclusion they sought—virtual certainty—and then worked backwards to find a figure that would lead to that conclusion. Mathematical gymnastics of this sort do not constitute "sufficient factual matter" to support a "plausible" allegation. *Ashcroft*, 556 U.S. at 678 (2009) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). And contrary to plaintiffs' efforts, the "speculative" reasoning foreclosed by *Clapper* cannot be avoided by dressing "a chain of possibilities" in the clothing of mathematical certainty when the calculation lacks a statistical basis. 133 S. Ct. at 1150.[23]

---

[22] *Id.* ("*even* if one assumes a 0.00000001% chance" that "the NSA [intercepts] any particular communication") (emphasis added).

[23] Plaintiffs' probability analysis also assumes that (i) the chance of interception for each communication is the same and (ii) the interception of one communication does not affect the

Furthermore, plaintiffs' allegation that interception of Wikimedia's communications is virtually certain fails for a more fundamental reason. Logically antecedent to plaintiffs' flawed statistical analysis are plaintiffs' speculative claims about Upstream surveillance based on limited knowledge of Upstream surveillance's technical features and "strategic imperatives." Pls. Opp. Br. at 17. In other words, the "virtual certainty" plaintiffs allege assumes that the NSA is *actually* using Upstream surveillance in the way plaintiffs suppose is necessary for that mode of surveillance to achieve the NSA's stated goals. As already discussed, although plaintiffs have alleged facts that plausibly establish that the NSA uses Upstream surveillance at some number of chokepoints, they have not alleged facts that plausibly establish that the NSA is using Upstream surveillance to copy all or substantially all communications passing through those chokepoints. In this regard, plaintiffs can only speculate, which *Clapper* forecloses as a basis for standing. Indeed, the Supreme Court in *Clapper* rejected the argument that standing could be based on a "very strong likelihood" that the NSA would "intercept at least some of plaintiffs' communications" based on speculation about the government's "motivat[ion]" to exercise its "capacity" for such interception. 133 S. Ct. at 1159 (Breyer, J. dissenting). Relying on a speculative foundation regarding how Upstream surveillance must operate, plaintiffs fail to allege that an injury is "real and immediate" rather than "conjectural or hypothetical." *Lyons*, 461 U.S. at 201. This is true regardless of how probable NSA interception of Wikimedia's

---

odds of any other communication's interception. In other words, plaintiffs assume that a communication from Syria has the same likelihood of being intercepted as a communication from Canada and that the fact that a communication from a Syrian computer has been intercepted has no bearing on the likelihood that a subsequent communication sent from the same computer in Syria will be intercepted. Moreover, plaintiffs provide no evidence of how many of Wikimedia's international Internet communications are transmitted to or from areas of the world in which interception is more likely.

communications would be if the NSA were *in fact* routinely using Upstream surveillance to intercept substantial quantities of text-based Internet communications.[24]

In the end, plaintiffs' standing argument boils down to suppositions about how Upstream surveillance *must* operate in order to achieve the government's stated goals. Of course, in a case like this, plaintiffs necessarily rely on probabilities and speculation because most facts about Upstream surveillance remain classified, and hence plaintiffs see through a glass darkly. Nevertheless, the speculative reasoning plaintiffs advance is not a basis for standing under *Clapper*. *See id.* at 1147-50. To see why this must be so, consider the risks of error at play on a threshold standing question. On the one hand, a court that does not find standing on the basis of probabilities and suppositions runs the risk of a false negative—closing the courthouse doors to a plaintiff who suffers an actual injury fairly traceable to the defendant. On the other hand, a court that bases standing on such speculation runs the risk of a false positive—proceeding in a litigation that is not a "Case[]" or "Controvers[y]" under Article III. U.S. Const. art. III, § 2, cl. 2. Obviously, both risks of error should be avoided where possible, but where, as here, a court is confronted with substantial uncertainty, the risk of a false positive is of greater concern because it implicates an existential question about the litigation—whether it is, in fact, a case or controversy—and the limits of the judiciary's power in relation to the other branches of

---

[24] Plaintiffs also cite a publicly disclosed NSA document, which states that "HTTP" is used in "nearly everything a typical user does on the Internet" and identifies Wikipedia (along with several other well-known websites) as an example of a source of HTTP communications. AC ¶ 107. But as defendants correctly point out, the document does not help to establish an injury to Wikimedia that is fairly traceable to Upstream surveillance because it neither identifies Upstream surveillance nor gives any indication that the NSA is actually collecting the communications of the websites listed.

government.[25] As the Supreme Court recognized in *Clapper*, this is especially true where, as here, "reaching the merits of the dispute would force [a court] to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional," particularly "in the fields of intelligence gathering and foreign affairs." *Clapper*, 133 S. Ct. at 1147. Thus, as *Clapper* dictates, standing cannot be established on the basis of mere speculation. *See id.* at 1147-50. Accordingly, plaintiffs in this case lack standing on that ground to challenge the NSA's use of Upstream surveillance.[26]

IV.

Plaintiffs further allege actual injury on the ground that Upstream surveillance undermines plaintiffs' ability to carry out activities crucial to their missions (i) by forcing them to take burdensome measures to minimize the chance that the confidentiality of their sensitive information will be compromised and (ii) by reducing the likelihood that individuals will share sensitive information with them. Attorney Dratel, for example, allegedly employed burdensome electronic security measures to protect his communications with his clients and, in some instances, travelled abroad to gather information in person.

The *Clapper* plaintiffs advanced indistinguishable arguments, and the Supreme Court flatly rejected them, explaining that the alleged injuries were not "fairly traceable to [Section

---

[25] *See Lujan*, 504 U.S. at 559-60 ("[T]he Constitution's central mechanism of separation of powers depends largely upon common understanding of what activities are appropriate to legislature, to executives, and to courts," which includes identifying cases "that are of the justiciable sort referred to in Article III").

[26] In addition to alleging that some of their communications are intercepted, plaintiffs allege a "substantial likelihood" that some of those communications must be retained, read, and disseminated by the NSA. AC ¶ 71. This allegation necessarily fails. Because plaintiffs have not plausibly alleged initial NSA interception of their text-based Internet communications, it follows that they have not adequately alleged that any of their communications are retained, read, or disseminated by the NSA.

702]" because (i) plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending" and (ii) plaintiffs cannot establish injury "based on third parties' subjective fear of surveillance." 133 S. Ct. at 1151, 1152 n.7.[27] Thus, *Clapper* controls here. The subjective fears of third parties and any alleged burdensome measures taken as a result of subjective fear of surveillance are not fairly traceable to Upstream surveillance, and therefore do not establish Article III standing.

V.

A final point, raised in *Clapper*, merits mention here: whether the standing requirement as applied in *Clapper* bids fair to immunize Section 702 and Upstream surveillance from judicial scrutiny. This concern is misplaced. To be sure, no government surveillance program should be immunized from judicial scrutiny, and indeed Section 702 and Upstream surveillance have no such immunity. As the *Clapper* majority noted, Section 702 surveillance is reviewed when: (i) the FISC reviews targeting and minimization procedures of general surveillance practices to ensure, *inter alia*, "the targeting and minimization procedures comport with the Fourth Amendment," (ii) criminal defendants prosecuted on the basis of Section 702 surveillance challenge the validity of that surveillance, and (iii) electronic communications service providers who are directed to assist the government in surveillance challenge the directives before the FISC. *Clapper*, 133 S. Ct. at 1154. Moreover, the recently enacted USA FREEDOM Act

---

[27] The amici curiae in this case argue that standing can be established on the ground that the alleged government surveillance chills speech protected by the First Amendment. *See* Br. of *Amici Curiae* American Booksellers Association, *et al.*, at 12-17; Br. of *Amici Curiae* First Amendment Scholars, at 9-19. As with plaintiffs' argument, the amici curiae's argument fails for the reasons articulated in *Clapper*. 133 S. Ct. at 1150-52. Both amicus briefs, which focus chiefly on the chilling argument, have been carefully reviewed and found unpersuasive. It is also worth noting that the only other nine individuals who cite their own works as frequently as do the nine authors of the First Amendment Scholars amicus brief are members of the Supreme Court, who, unlike the amici, do so out of sheer necessity.

provides that amicus curiae may be appointed to represent the public in certain FISC proceedings involving NSA surveillance pursuant to Section 702. Pub. L. No. 114-23, 129 Stat. 268, 279.[28] These examples, of course, are not civil challenges to Section 702, and establishing standing to challenge Section 702 in a civil case is plainly difficult. But such difficulty comes with the territory. It is not a flaw of a classified program that standing to challenge that program is not easily established; it is a constitutional requirement essential to separation of powers.

VI.

For the reasons stated here, defendants' motion to dismiss is granted.

An appropriate Order will issue.

Alexandria, Virginia
October 23, 2015

/s/
T. S. Ellis, III
United States District Judge

[28] It should also be remembered that the classified program at issue here is authorized by a law that was passed through the democratic process. Should society's suspicions about surveillance programs rise to a level sufficient to cause citizens to suspect Orwellian harms that outweigh the benefits to national security, surveillance programs can be revised or eliminated the same way they were authorized, namely through the legislative process. It is also possible that the jurisprudence of constitutional standing may change in the future.