PUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 15-2560

WIKIMEDIA FOUNDATION; NATIONAL ASSOCIATION OF CRIMINAL DEFENSE ATTORNEYS; HUMAN RIGHTS WATCH; PEN AMERICAN CENTER; GLOBAL FUND FOR WOMEN; THE NATION MAGAZINE; THE RUTHERFORD INSTITUTE; WASHINGTON OFFICE ON LATIN AMERICA; AMNESTY INTERNATIONAL USA,

Plaintiffs − Appellants,

v.

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE; ADMIRAL MICHAEL S. ROGERS, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service; OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE; DANIEL R. COATS, in his official capacity as Director of National Intelligence; DEPARTMENT OF JUSTICE; JEFFERSON B. SESSIONS III, in his official capacity as Attorney General of the United States,

Defendants – Appellees.

COMPUTER SCIENTISTS AND TECHNOLOGISTS; REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS; THE THOMAS JEFFERSON CENTER FOR THE PROTECTION OF FREE EXPRESSION; AMERICAN SOCIETY OF NEWS EDITORS; ASSOCIATION OF ALTERNATIVE NEWSMEDIA; FIRST AMENDMENT COALITION; FIRST LOOK MEDIA, INC.; FREE PRESS; FREEDOM OF THE PRESS FOUNDATION; GATEHOUSE MEDIA; INTERNATIONAL DOCUMENTARY ASSOCIATION; INVESTIGATIVE REPORTERS AND EDITORS, INCORPORATED; INVESTIGATIVE REPORTING WORKSHOP AT AMERICAN UNIVERSITY; THE MEDIA CONSORTIUM; NATIONAL PRESS PHOTOGRAPHERS ASSOCIATION; NORTH JERSEY MEDIA GROUP, INCORPORATED; ONLINE NEWS ASSOCIATION; RADIO TELEVISION DIGITAL NEWS

ASSOCIATION; REPORTERS WITHOUT BORDERS; TULLY CENTER FOR FREE SPEECH; UNITED STATES JUSTICE FOUNDATION; FREE SPEECH DEFENSE AND EDUCATION FUND; FREE SPEECH COALITION; WESTERN JOURNALISM CENTER; GUN OWNERS OF AMERICA, INC.; GUN OWNERS FOUNDATION; DOWNSIZE DC FOUNDATION; DOWNSIZEDC.ORG; CONSERVATIVE LEGAL DEFENSE AND EDUCATION FUND; INSTITUTE ON THE CONSTITUTION; POLICY ANALYSIS CENTER; LAW PROFESSORS; ELECTRONIC FRONTIER FOUNDATION; FIRST AMENDMENT LEGAL SCHOLARS,

Amici Supporting Appellants.

Appeal from the United States District Court for the District of Maryland, at Baltimore. T. S. Ellis, III, Senior District Judge. (1:15−cv−00662−TSE)

Argued: December 8, 2016 Decided: May 23, 2017

Before MOTZ and DIAZ, Circuit Judges, and DAVIS, Senior Circuit Judge.

Affirmed in part, vacated in part, and remanded by published opinion. Judge Diaz wrote the opinion, in which Judge Motz joined and in which Senior Judge Davis joined in part. Senior Judge Davis wrote a separate opinion dissenting in part.

ARGUED: Patrick Christopher Toomey, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, New York, New York, for Appellants. Catherine H. Dorsey, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C., for Appellees. **ON BRIEF:** Jameel Jaffer, Alexander Abdo, Ashley Gorski, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, New York, New York; Deborah A. Jeon, David R. Rocah, AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND, Baltimore, Maryland; Charles S. Sims, David A. Munkittrick, PROSKAUER ROSE LLP, New York, New York, for Appellants. Benjamin C. Mizer, Principal Deputy Assistant Attorney General, Douglas N. Letter, H. Thomas Byron III, Michael Shih, Civil Division, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C.; Rod J. Rosenstein, United States Attorney, OFFICE OF THE UNITED STATES ATTORNEY, Baltimore, Maryland, for Appellees. Jennifer Stisa Granick, Director of Civil Liberties, Center for Internet and Society, STANFORD LAW SCHOOL, Stanford, California; Matthew J. Craig, SHAPIRO ARATO LLP, New York, New York, for Amicus Computer Scientists

and Technologists. Margot E. Kaminski, Assistant Professor of Law, Moritz College of Law, THE OHIO STATE UNIVERSITY, Columbus, Ohio; Chelsea J. Crawford, Joshua R. Treem, BROWN, GOLDSTEIN & LEVY, LLP, Baltimore, Maryland, for Amicus First Amendment Legal Scholars. J. Joshua Wheeler, Thomas Jefferson Center for the Protection of Free Expression and First Amendment Clinic, THE UNIVERSITY OF VIRGINIA SCHOOL OF LAW, Charlottesville, Virginia; Bruce D. Brown, Gregg P. Leslie, Hannah Bloch-Wehba, REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS, Washington, D.C.; Peter Scheer, FIRST AMENDMENT COALITION, San Rafael, California; Lynn Oberlander, General Counsel, Media Operations, FIRST LOOK MEDIA, INC., New York, New York; Matthew F. Wood, FREE PRESS, Washington, D.C.; Polly Grunfeld Sack, SVP, General Counsel and Secretary, GATEHOUSE MEDIA, LLC, Pittsford, New York; Jennifer A. Borg, General Counsel, NORTH JERSEY MEDIA GROUP, INCORPORATED, Woodland Park, New Jersey, for Amici Reporters Committee for Freedom of the Press, The Thomas Jefferson Center for the Protection of Free Expression, American Society of News Editors, Association of Alternative Newsmedia, First Amendment Coalition, First Look Media, Inc., Free Press, Freedom of the Press Foundation, Gatehouse Media, International Documentary Association, Investigative Reporters and Editors, Incorporated, Investigative Reporting Workshop at American University, The Media Consortium, National Press Photographers Association, North Jersey Media Group, Incorporated, Online News Association, Radio Television Digital News Association, Reporters Without Borders, and Tully Center for Free Speech. Kevin M. Goldberg, FLETCHER, HEALD & HILDRETH, PLC, Arlington, Virginia, for Amici American Society of News Editors and Association of Alternative Newsmedia. Marcia Hofmann, ZEITGEIST LAW PC, San Francisco, California, for Amicus Freedom of the Press Foundation. Mickey H. Osterreicher, Buffalo, New York, for Amicus National Press Photographers Association. Laura R. Handman, Alison Schary, Washington, D.C., Thomas R. Burke, DAVIS WRIGHT TREMAINE LLP, San Francisco, California, for Amicus Online News Association. Kathleen A. Kirby, WILEY REIN LLP, Washington, D.C., for Amicus Radio Television Digital News Association. Michael Connelly, UNITED STATES JUSTICE FOUNDATION, Ramona, California, for Amicus United States Justice Foundation. Robert J. Olson, Herbert W. Titus, William J. Olson, Jeremiah L. Morgan, WILLIAM J. OLSON, P.C., Vienna, Virginia, for Amici United States Justice Foundation, Free Speech Defense and Education Fund, Free Speech Coalition, Western Journalism Center, Gun Owners of America, Inc., Gun Owners Foundation, Downsize DC Foundation, DownsizeDC.org, Conservative Legal Defense and Education Fund, Institute on the Constitution, and Policy Analysis Center. Adam Steinman, Professor of Law, UNIVERSITY OF ALABAMA SCHOOL OF LAW, Tuscaloosa, Alabama, for Amicus Law Professors. Sophia Cope, Mark Rumold, Andrew Crocker, Jaime Williams, ELECTRONIC FRONTIER FOUNDATION, San Francisco, California, for Amicus Electronic Frontier Foundation.

DIAZ, Circuit Judge:

The Wikimedia Foundation and eight other organizations appeal the dismissal of their complaint challenging Upstream surveillance, an electronic surveillance program operated by the National Security Agency (the "NSA"). The district court, relying on the discussion of speculative injury from *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013), held that the allegations in the complaint were too speculative to establish Article III standing. We conclude that *Clapper*'s analysis of speculative injury does not control this case, since the central allegations here are not speculative. Accordingly, as for Wikimedia, we vacate and remand because it makes allegations sufficient to survive a facial challenge to standing. As for the other Plaintiffs, we affirm because the complaint does not contain enough well-pleaded facts entitled to the presumption of truth to establish their standing.

I.

A.

Before diving into the details of Plaintiffs' complaint, we provide an overview of the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1801 *et seq.*, the statute from which the government derives its authority to conduct Upstream surveillance.

Congress enacted FISA in 1978 to regulate electronic surveillance undertaken to gather foreign intelligence information. David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* § 3:8 (2d ed.), Westlaw (database updated Aug. 2016) (hereinafter Kris & Wilson); *see also* 50 U.S.C. § 1801 (defining electronic

surveillance). FISA created two specialized courts—the Foreign Intelligence Surveillance Court (the "FISC"), from which the government generally must obtain authorization before conducting electronic surveillance, and the Foreign Intelligence Surveillance Court of Review, which has jurisdiction to review the denial of a FISA application for electronic surveillance. Kris & Wilson § 5:1. As originally enacted, FISA required the government to demonstrate probable cause to believe that the target of its surveillance was "a foreign power or an agent of a foreign power," and that the facility or place at which surveillance would be directed was "being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(a)(2); *see also* Kris & Wilson § 7:2.

"Until 2008, FISA applied only to investigative conduct inside the United States." Kris & Wilson § 4:2. That changed through the FISA Amendments Act of 2008, which authorized the government to acquire foreign-intelligence information by targeting for up to one year non-U.S. persons reasonably believed to be abroad. *See* 50 U.S.C. § 1881a. FISA Section 702, 50 U.S.C. § 1881a, sets forth the process for obtaining that authority.

Generally, the Attorney General and the Director of National Intelligence initiate the process by submitting a "certification" regarding the proposed surveillance to the FISC for approval. *Id.* § 1881a(g)(1)(A). That certification must attest, inter alia, that:

> (1) procedures are in place "that . . . are reasonably designed" to ensure that an acquisition is "limited to targeting persons reasonably believed to be located outside" the United States; (2) minimization procedures adequately restrict the acquisition, retention, and dissemination of nonpublic information about unconsenting U.S. persons . . .; (3) guidelines have been adopted to ensure compliance with targeting limits and the Fourth

> Amendment; and (4) the procedures and guidelines . . . comport with the Fourth Amendment.

Clapper, 133 S. Ct. at 1145 (quoting 50 U.S.C. § 1881a(g)(2)).

The FISC reviews the certification to ensure that it contains the statutorily required elements and has targeting and minimization procedures that are both consistent with the Fourth Amendment and are "reasonably designed" to meet certain requirements. *Id.* In particular, the FISC must find that the targeting procedures are "reasonably designed" to: (i) ensure that acquisition "is limited to targeting persons reasonably believed to be located outside the United States," and (ii) "prevent the intentional acquisition of" wholly domestic communications. 50 U.S.C. § 1881a(i)(2)(B). The FISC must also find that the minimization procedures are "reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." *Id.* § 1801(h)(1); *see id.* § 1881a(i)(2)(C) (referring to § 1801(h)).

Section 702 prohibits the intentional targeting of "any person known at the time of acquisition to be located in the United States," *id.* § 1881a(b), but allows the government to intercept communications between a U.S. person inside the country and a foreigner abroad targeted by intelligence officials, *see id.* § 1881a(a)–(b); *see also* Kris & Wilson § 17:5. Furthermore, surveillance under Section 702 may be conducted for purposes other than counterterrorism—the statute defines "foreign intelligence information" to

mean, among other things, information that relates to "the conduct of the foreign affairs of the United States," 50 U.S.C. § 1801(e)(2)(B)—and the government need not identify "the specific facilities, places, premises, or property at which" it will direct surveillance, *id.* § 1881a(g)(4).

The absence of particularity and probable cause requirements in Section 702 surveillance allows the government to monitor the communications of thousands of individuals and groups under a single FISC Order. *See* Office of the Director of National Intelligence, *Calendar Year 2014 Statistical Transparency Report* 1–2 (2015) (stating that in 2014 the government used its authority pursuant to Section 702 to target an estimated 92,707 persons, groups, and entities under one FISC Order).[1] Furthermore, the minimization procedures allow the government to retain communications—including those of U.S. persons—if the government concludes that they contain "foreign intelligence" information. *See* Kris & Wilson §§ 9:5, 17:5.

The government has acknowledged that it conducts two forms of surveillance under Section 702—PRISM and Upstream. *See* Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 7 (2014) (hereinafter PCLOB Report).[2] Only Upstream is at issue here. Though the government has disclosed some information about

[1] Plaintiffs' complaint incorporates this document.

[2] Plaintiffs' complaint incorporates this report.

Upstream, most technical details of the surveillance process remain classified. *See Jewel v. Nat'l Sec. Agency*, 810 F.3d 622, 627 (9th Cir. 2015).

B.

In June 2015, Plaintiffs—educational, legal, human rights, and media organizations—filed their first amended complaint wherein they ask for, among other things, a declaration that Upstream surveillance violates the First and Fourth Amendments, an order permanently enjoining the NSA from conducting Upstream surveillance, and an order directing the NSA "to purge all records of Plaintiffs' communications in their possession obtained pursuant to Upstream surveillance." J.A. 84.

Plaintiffs make two central allegations. First, in what we refer to as the Wikimedia Allegation, Wikimedia alleges that "the sheer volume of [its] communications makes it virtually certain that the NSA has intercepted, copied, and reviewed at least some of [its] communications."[3] J.A. 46. Second, in what we refer to as the Dragnet Allegation, all nine Plaintiffs allege that in the course of conducting Upstream surveillance the NSA is "intercepting, copying, and reviewing substantially all" text-based communications entering and leaving the United States, including their own. J.A. 46. After setting forth supporting background relevant to each, we describe the Wikimedia and Dragnet Allegations.

[3] Though all nine Plaintiffs made this allegation, only Wikimedia pursues it on appeal.

1.

Plaintiffs allege that "Upstream surveillance involves the NSA's seizing and searching the [I]nternet communications of U.S. citizens and residents en masse as those communications travel across the [I]nternet 'backbone' in the United States." J.A. 40. "The [I]nternet backbone is the network of high-capacity cables, switches, and routers [administered by telecommunications-service providers] that facilitates both domestic and international communication via the [I]nternet." J.A. 40. It includes "the approximately 49 international submarine cables that carry [I]nternet communications into and out of the United States and that land at approximately 43 different points within the country." J.A. 42.

The NSA performs Upstream surveillance by first identifying a target and then identifying "selectors" for that target. Selectors are the specific means by which the target communicates, such as e-mail addresses or telephone numbers. Selectors cannot be keywords (e.g., "bomb") or names of targeted individuals (e.g., "Bin Laden").

The NSA then "tasks" selectors for collection and sends them to telecommunications-service providers. Those providers must assist the government in intercepting communications to, from, or "about" the selectors. "About" communications are those that contain a tasked selector in their content, but are not to or from the target. "For instance, a communication between two third parties might be acquired because it contains a targeted email address in the body of the communication." PCLOB Report at 119.

We note an important distinction between Internet transactions and Internet communications. While Upstream surveillance "is intended to acquire Internet *communications*, it does so through the acquisition of Internet *transactions*." PCLOB Report at 39. An example illustrates the point. When an individual sends an email on the Internet, the message is broken up into one or more "data packets" which are transmitted across the Internet backbone to their destination and, upon arrival, reassembled by the recipient's computer to reconstruct the communication. The individual data packets generated by a single email can take "different routes [across the backbone] to their common destination." PCLOB Report at 125. Relatedly, when two people communicate, the data packets from the target can take a different path along the backbone than the data packets to the target. "The government describes an Internet 'transaction' as 'a complement of packets traversing the Internet that together may be understood by a device on the Internet and, where applicable, rendered in an intelligible form to the user of that device.'" *Redacted*, 2011 WL 10945618, at *9 n.23 (FISA Ct. Oct. 3, 2011) (quoting a government submission to the FISC).[4] An Internet transaction can comprise one or many discrete communications.

"To identify and acquire Internet transactions associated with the Section 702-tasked selectors on the Internet backbone, Internet transactions are first filtered to eliminate potential domestic transactions, and then are screened to capture only transactions containing a tasked selector. Unless transactions pass both these screens,

[4] Plaintiffs' complaint incorporates this FISC opinion.

they are not ingested into government databases." PCLOB Report at 37. "If a single discrete communication within [a multi-communication transaction] is to, from, or about a Section 702-tasked selector, and at least one end of the transaction is foreign, the NSA will acquire the entire [multi-communication transaction]." PCLOB Report at 39. Once acquired, communications are subject to FISC-approved minimization procedures. The NSA's minimization procedures, for example, limit the types of queries that analysts can conduct across data sets of Section 702-acquired information.

Plaintiffs allege that Upstream surveillance works in practice as follows. First, the NSA copies "substantially all international text-based communications—and many domestic ones—flowing across certain high-capacity cables, switches, and routers" by "[u]sing surveillance devices installed at key access points along the [I]nternet backbone." J.A. 43. Second, it "attempts to filter out and discard some wholly domestic communications," though that effort "is incomplete." J.A. 43. Third, it reviews the full content of the copied communications for targeted selectors, including IP addresses. J.A. 43. Finally, it "retains [and with few restrictions analyzes] all communications that contain selectors associated with its targets, as well as those that happen to be bundled with them in transit." J.A. 44.

2.

Wikimedia asserts that the NSA is intercepting, copying, and reviewing at least some of its communications in the course of Upstream surveillance, "even if the NSA conducts Upstream surveillance on only a single [I]nternet backbone link." J.A. 49. Wikimedia, "the operator of one of the most-visited websites in the world," alleges that it

"engages in more than one trillion international communications each year, with individuals who are located in virtually every country on earth." J.A. 56. According to Wikimedia, Upstream surveillance implicates three categories of its communications: (1) communications with its community members; (2) internal "log" communications, which include users' IP addresses and the URLs of webpages sought by users; and (3) communications between its staff and individuals around the world. J.A. 55–56.

Wikimedia further alleges that "[g]iven the relatively small number of international chokepoints,"[5] the volume of its communications, and the geographical diversity of the people with whom it communicates, its "communications almost certainly traverse every international backbone link connecting the United States with the rest of the world." J.A. 47–48. And, Wikimedia alleges, "in order for the NSA to reliably obtain communications to, from, or about its targets in the way it has described, the government must be copying and reviewing all the international text-based communications that travel across a given link." J.A. 48.

That last allegation is so, says Wikimedia, because "as a technical matter, the government cannot know beforehand which communications will contain selectors associated with its targets, and therefore it must copy and review all international text-based communications transiting [a] circuit in order to identify those of interest." J.A. 48. That is because data packets that constitute a communication "travel independently

[5] By "chokepoint," Wikimedia refers to the 49 international submarine cables and the "limited number" of terrestrial cables that carry Internet communications into and out of the United States. J.A. 47–48.

of one another, intermingled with packets of other communications in the stream of data," and "the packets of interest cannot be segregated from other, unrelated packets in advance." J.A. 49. Thus, the NSA must "copy *all* such packets traversing a given backbone link, so that it can reassemble and review the transiting communications." J.A. 49.

Tying these allegations together, Wikimedia asserts that if the NSA is monitoring a single [I]nternet backbone link, then the NSA is intercepting, copying, and reviewing at least some of Wikimedia's communications. According to Wikimedia, "the NSA has confirmed that it conducts Upstream surveillance at more than one point along the [I]nternet backbone." J.A. 49. In addition to the PCLOB Report's confirmation of the program's existence, Wikimedia points to a purported NSA slide which shows that a single telecommunications-service provider is facilitating Upstream surveillance at "seven major international chokepoints in the United States" and a purported NSA document which states that the NSA is expending significant resources to "create collection/processing capabilities at many of the chokepoints operated by U.S. providers." J.A. 50–51.

Wikimedia has "an acute privacy interest in its communications" because its "mission and existence depend on its ability to ensure that readers and editors can explore and contribute to [its websites] privately when they choose to do so." J.A. 59–60. It has, in response to Upstream surveillance, taken burdensome steps to protect "the privacy of its communications and the confidentiality of the information it thereby receives." J.A.

60–61. Among other things, Wikimedia has "self-censor[ed] communications or forgo[ne] electronic communications altogether." J.A. 64.

Finally, the first amended complaint alleges that "even if one assumes a 0.00000001% chance . . . of the NSA copying and reviewing any particular communication, 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%." J.A. 46–47. This is an extension of the allegation that Wikimedia engages in more than one trillion international communications each year.

3.

In the Dragnet Allegation, Plaintiffs say that "given the way the government has described Upstream surveillance, it has a strong incentive to intercept communications at as many backbone chokepoints as possible." J.A. 49. Thus, "[i]f 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." J.A. 50.

Plaintiffs allege that the nature of online communication, including that data packets to a target can take different routes than data packets from a target, makes this conclusion "especially true." J.A. 50. They also incorporate into their complaint a *New York Times* article asserting that the NSA "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." J.A. 51.

Furthermore, Plaintiffs often communicate with individuals whom the NSA is likely to target through Upstream surveillance, and "[a] significant amount of the information that [they] exchange over the [I]nternet is 'foreign intelligence information.'" J.A. 52. "Because of ongoing government surveillance, including Upstream surveillance, Plaintiffs have had to take burdensome and sometimes costly measures to" protect "the confidentiality of their sensitive information." J.A. 52. Upstream surveillance compels them to censor their own communications and, in some instances, to forgo electronic communications altogether.

Finally, Joshua Dratel, a member of Plaintiff National Association of Criminal Defense Lawyers, also challenges Upstream surveillance. One of Dratel's clients "has received notice of [Section 702 surveillance], and [Dratel] previously represented a client in another case where officials have told Congress that the government used [Section 702 surveillance] in the course of its investigation." J.A. 68–69.

C.

The government moved to dismiss for lack of standing and submitted evidence, including declarations by Robert Lee and Alan Salzberg. The Lee Declaration challenges Plaintiffs' assertion that, as a technical matter, the NSA must be copying all data packets that traverse a given backbone link. The Salzberg Declaration attacks Plaintiffs' probability calculation that there's a greater than 99.9999999999% chance that the NSA is copying and reviewing their communications.

The district court, relying on *Clapper*, held that Plaintiffs had failed to establish standing because their allegations "depend on suppositions and speculation, with no basis

in fact, about how the NSA implements Upstream surveillance." J.A. 190. The court characterized the government's motion as a facial challenge, and thus did not consider either declaration. Because so much of the district court's opinion depends on *Clapper*, we summarize that case first.

1.

In *Clapper*, plaintiffs (including six of the nine Plaintiffs here, but not including Dratel or Wikimedia) lodged a facial challenge to Section 702 on the day that the law went into effect, seeking declaratory and injunctive relief. 133 S. Ct. at 1145–46. They alleged that their work required them to "engage in sensitive and sometimes privileged telephone and e-mail communications with . . . individuals located abroad" who were "likely targets of surveillance under" Section 702. *Id.* at 1145. Plaintiffs had two separate theories of Article III standing: (1) there was an "objectively reasonable likelihood" that their communications would be intercepted in the future pursuant to Section 702 surveillance, and (2) they were forced to undertake costly and burdensome measures to avoid a substantial risk of surveillance. *Id.* at 1146. They did not, however, have "actual knowledge of the Government's [Section 702] targeting practices." *Id.* at 1148.

The Supreme Court held that neither injury established standing at the summary judgment stage. The theory of standing based on interception of communications "relie[d] on a highly attenuated chain of possibilities, [which did] not satisfy the requirement that threatened injury must be certainly impending." *Id.* at 1147–48. The Court broke the speculative chain into five parts:

> (1) the Government will decide to target the communications of non-U.S. persons with whom [plaintiffs] communicate; (2) in doing so, the Government will choose to invoke its authority under [Section 702] rather than utilizing another method of surveillance; (3) the Article III judges who serve on the [FISC] will conclude that the Government's proposed surveillance procedures satisfy [Section 702's] many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of [plaintiffs'] contacts; and (5) [plaintiffs] will be parties to the particular communications that the Government intercepts.

Id. at 1148.

"[A]t the summary judgment stage," the Court noted, plaintiffs "can no longer rest on mere allegations [to establish standing], but must set forth by affidavit or other evidence specific facts." *Id.* at 1148–49 (alteration and internal quotation marks omitted). The *Clapper* plaintiffs, however, had no "specific facts demonstrating that the communications of their foreign contacts w[ould] be targeted." *Id.* at 1149.

The assertion of harm based on measures taken to avoid surveillance also didn't suffice. Because "the harm [plaintiffs] s[ought] to avoid [wa]s not certainly impending," the Court explained, they couldn't "manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm." *Id.* at 1151. In other words, plaintiffs had failed to show that "[a]ny ongoing injuries" they were suffering were "fairly traceable" to Section 702 surveillance. *Id.* The Court suggested, however, that a lawyer who represented a target of Section 702 surveillance might have standing. *Id.* at 1154.

2.

Applying these principles, the district court in this case reasoned that while

> more is known about the nature and capabilities of NSA surveillance than was known at the time of *Clapper*, . . . no more is known about whether Upstream surveillance *actually* intercepts all or substantially all international text-based Internet communications, including plaintiffs' communications. . . . 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*.

J.A. 192. The court supported that conclusion with two observations relevant here: (1) it is unclear whether the NSA is "using [its] surveillance equipment to its full potential" to intercept "all communications passing through" chokepoints upon which the NSA has installed surveillance equipment, and (2) "the fact that all NSA surveillance practices must survive FISC review . . . suggests that the NSA is not using its surveillance equipment to its full potential." J.A. 190–91.

The district court also rejected the argument that *Clapper* "does not control here because plaintiffs are different from the *Clapper* plaintiffs." J.A. 194. The court focused on Dratel and Wikimedia. With respect to Dratel, the court concluded that the allegations failed to "plausibly establish that the information gathered from the two instances of Section 702 surveillance was the product of Upstream surveillance," and that it "appears substantially more likely that PRISM collection was used in [those] cases." J.A. 195.

As for Wikimedia, the court found that "the statistical analysis on which the argument rests [(i.e., the probability calculation that there's a greater than 99.9999999999% chance that the NSA is copying and reviewing Wikimedia's

communications)] is incomplete and riddled with assumptions," and that "[l]ogically 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.'"[6] *See* J.A. 197–99.

From the district court's dismissal of their complaint for lack of standing, Plaintiffs appeal.

II.

We review the district court's decision de novo, *Columbia Gas Transmission Corp. v. Drain*, 237 F.3d 366, 369 (4th Cir. 2001), and proceed as follows. First, we lay out the framework for deciding whether a plaintiff has established standing at the motion-to-dismiss stage. Then, we review the Wikimedia and Dragnet Allegations to see whether either establishes standing. We conclude that the Wikimedia Allegation does and the Dragnet Allegation does not.

A.

1.

Article III of the Constitution limits the jurisdiction of federal courts to "Cases" and "Controversies." U.S. Const. art. III, § 2. "The doctrine of standing gives meaning to these constitutional limits by 'identify[ing] those disputes which are appropriately

[6] The "speculative claims" that the court referred to all relate to Wikimedia's allegation that the NSA is "using Upstream surveillance to copy all or substantially all communications passing through" chokepoints which the NSA surveils. J.A. 199.

resolved through the judicial process.'" *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) (alteration in original) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)). To establish standing, a plaintiff must show: (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. *Id.*

"To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016) (quoting *Lujan*, 504 U.S. at 560). "For an injury to be particularized, it must affect the plaintiff in a personal and individual way." *Id.* (internal quotation marks omitted). "The fact that an injury may be suffered by a large number of people does not of itself make that injury a nonjusticiable generalized grievance." *Id.* at 1548 n.7. The purpose of the imminence requirement "is to ensure that the alleged injury is not too speculative for Article III purposes." *Clapper*, 133 S. Ct. at 1147. The "threatened injury must be *certainly impending* to constitute injury in fact, and . . . [a]llegations of *possible* future injury are not sufficient." *Id.* (second alteration in original) (internal quotation marks omitted).

"[E]ach element [of standing] 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 of the litigation." *Lujan*, 504 U.S. at 561. "A defendant may challenge [standing at the motion-to-dismiss stage] in one of two ways: facially or factually." *Beck v. McDonald*, 848 F.3d 262, 270 (4th Cir. 2017). In a

facial challenge, the defendant contends that the complaint "fails to allege facts upon which [standing] can be based," and the plaintiff "is afforded the same procedural protection" that exists on a motion to dismiss. *Adams v. Bain*, 697 F.2d 1213, 1219 (4th Cir. 1982). In a factual challenge, the defendant contends "that the jurisdictional allegations of the complaint [are] not true." *Id.* In that event, a trial court may look beyond the complaint "and in an evidentiary hearing determine if there are facts to support the jurisdictional allegations." *Id.*

"To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, 'to state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). We accept as true all well-pleaded facts in a complaint and construe them in the light most favorable to the plaintiff. *SD3, LLC v. Black & Decker (U.S.) Inc.*, 801 F.3d 412, 422 (4th Cir. 2015). Indeed, a court cannot "favor[] its perception of the relevant events over the narrative offered by the complaint," thereby "recasting 'plausibility' into 'probability.'" *Id.* at 430. However, legal conclusions pleaded as factual allegations, "unwarranted inferences," "unreasonable conclusions," and "naked assertions devoid of further factual enhancement" are not entitled to the presumption of truth. *Id.* at 422.

2.

The Third Circuit recently applied many of these principles in *Schuchardt v. President of the United States*, where it held that, "at least as a facial matter," a complaint challenging PRISM surveillance—the other form of publicly acknowledged Section 702

surveillance—"plausibly stated an injury in fact" sufficient to establish standing. 839 F.3d 336, 338 (3d Cir. 2016). Under PRISM surveillance, the government purportedly obtains "user communications exchanged using services provided by several large U.S. companies" directly from those companies' servers. *Id.* at 340.

Schuchardt's central allegation was that the NSA is "intercepting, monitoring and storing the content of all or substantially all of the e-mail sent by American citizens, [and thus] his own online communications had been seized in the dragnet." *Id.* at 341 (emphasis omitted). In support of that allegation, Schuchardt stated that he used online services targeted by PRISM surveillance and incorporated into his complaint "excerpts of the classified materials" made public through newspaper articles and filings in other cases. *Id.* at 341. The complaint and its exhibits described the "technical means through which PRISM purportedly achieves a nationwide email dragnet" and were "replete with details confirming PRISM's operational scope and capabilities." *Id.* at 350.

For example, a slide from a purported NSA presentation "identif[ied] company names and the dates they began cooperating with" the NSA, while another exhibit "indicate[d] . . . that the degree of access those providers granted enables the Government to query their facilities at will for 'real-time interception of an individual's [I]nternet activity.'" *Id.* at 349–50 (citations omitted). Another purported NSA slide "confirm[ed] that—consistent with a dragnet capturing 'all or substantially all of the e–mail sent by American citizens'—the scale of the data collected by PRISM is so vast that the Government reported difficulty processing it according 'to the norms' to which [it has] become accustomed." *Id.* at 350 (alteration in original) (citations omitted).

The Third Circuit bifurcated its analysis. First, it found Schuchardt's allegations sufficiently particularized to satisfy the injury-in-fact requirement. *Id.* at 345–46. Though PRISM surveillance is "universal in scope," the harm that Schuchardt alleged was "unmistakably personal"—"he ha[d] a constitutional right to maintain the privacy of his personal communications, online or otherwise." *Id.* Moreover, "the fact that [many others] may share a similar interest d[id] not change [the injury's] individualized nature because Schuchardt's allegations ma[de] clear that he [wa]s among the persons" targeted by PRISM. *Id.* at 346 (internal quotation marks omitted).

Second, the court credited Schuchardt's allegations as true for the purpose of resolving the facial challenge to his complaint. *Id.* at 346–50. The level of detail in the complaint—sufficient to describe "the technical means through which PRISM purportedly" functions and to "confirm[] PRISM's operational scope and capabilities"—made his allegation about "the Government's virtual dragnet" plausible. *Id.* at 349–50. In doing so, the Third Circuit made clear that Schuchardt's reliance on exhibits was not disfavored, and that "[d]espite *Clapper*'s observation that the standing inquiry is 'especially rigorous' in matters touching on 'intelligence gathering and foreign affairs,'" it knew of no instance where a court had "imposed a heightened pleading standard for cases implicating national security," and thus "assume[d] without deciding that" one did not apply. *Id.* at 348 n.8, 348–49 (quoting *Clapper*, 133 S. Ct. at 1147).

We find the Third Circuit's approach persuasive and bifurcate our analyses of the Wikimedia and Dragnet Allegations in similar fashion.

B.

1.

As a reminder, the Wikimedia Allegation is that the NSA is intercepting, copying, and reviewing at least some of Wikimedia's communications in the course of Upstream surveillance, "even if the NSA conducts Upstream surveillance on only a single [I]nternet backbone link." J.A. 49.

We conclude that this allegation satisfies the three elements of Article III standing. We begin with injury in fact. *See Spokeo*, 136 S. Ct. at 1548 (defining injury in fact as the invasion of a legally protected interest that is concrete and particularized and actual or imminent). The allegation that the NSA is intercepting and copying communications suffices to show an invasion of a legally protected interest—the "Fourth Amendment right to be free from unreasonable searches and seizures." *Schuchardt*, 839 F.3d at 353; *see also Am. Civil Liberties Union v. Clapper*, 785 F.3d 787, 801 (2d Cir. 2015) (holding at motion-to-dismiss stage that complaint challenging NSA's bulk telephone metadata collection program established standing to assert a Fourth Amendment violation where alleged injury was "collection, and maintenance in a government database, of records relating to" plaintiffs).

The injury is also concrete and particularized, despite "[t]he fact that [it is] suffered by a large number of people," because Wikimedia says that the NSA is seizing its own communications through Upstream surveillance. *See Spokeo*, 136 S. Ct. at 1548 n.7; *accord Schuchardt*, 839 F.3d at 346. And, finishing up with the injury-in-fact element, the injury "is not too speculative for Article III purposes." *Clapper*, 133 S. Ct.

at 1147. Indeed, there's nothing speculative about it—the interception of Wikimedia's communications is an actual injury that has already occurred.

The Wikimedia Allegation also satisfies the other two elements of Article III standing. Upstream surveillance is the direct cause of the alleged injury, and there's no reason to doubt that the requested injunctive and declaratory relief would redress the harm. *See Lujan*, 504 U.S. at 560–61 (providing that the injury must be "fairly traceable" to the conduct complained of and "likely" to be redressed by a favorable decision).

However, just because this allegation satisfies the elements of Article III standing doesn't mean that we must accept it as true for the purpose of resolving the government's facial challenge to the complaint. Thus, we proceed to the second part of our analysis to decide whether the Wikimedia Allegation is plausible.

Wikimedia alleges three key facts that are entitled to the presumption of truth. First, "[g]iven the relatively small number of international chokepoints," the volume of Wikimedia's communications, and the geographical diversity of the people with whom it communicates, Wikimedia's "communications almost certainly traverse every international backbone link connecting the United States with the rest of the world." J.A. 47–48.[7]

[7] On appeal, Wikimedia attempts to rephrase this allegation so that it reads, "Wikimedia's communications traverse every major [I]nternet circuit entering or leaving the United States." Appellants' Br. at 24. We look, however, to the wording of the complaint. That said, the plausibility pleading regime doesn't automatically invalidate allegations that contain probabilistic-sounding words. For the purpose of deciding whether the Wikimedia Allegation is plausible, we find this supporting allegation, based as it is upon other factual allegations, to be well-pleaded. Indeed, Wikimedia need only (Continued)

Second, "in order for the NSA to reliably obtain communications to, from, or about its targets in the way it has described, the government," for technical reasons that Wikimedia goes into at length, "must be copying and reviewing all the international text-based communications that travel across a given link" upon which it has installed surveillance equipment. J.A. 48. Because details about the collection process remain classified, Wikimedia can't precisely describe the technical means that the NSA employs. Instead, it spells out the technical rules of how the Internet works and concludes that, given that the NSA is conducting Upstream surveillance on a backbone link, the rules require that the NSA do so in a certain way.

We would never confuse the plausibility of this conclusion with that accorded to Newton's laws of motion. But accepting the technical rules about the Internet as true, and given that Wikimedia is applying them in an appropriate context (i.e., it uses the rules to explain the technical means through which Upstream surveillance functions), we find this conclusion reasonable and entitled to the presumption of truth.

Third, per the PCLOB Report and a purported NSA slide, "the NSA has confirmed that it conducts Upstream surveillance at more than one point along the [I]nternet backbone." J.A. 49–51. Together, these allegations are sufficient to make plausible the conclusion that the NSA is intercepting, copying, and reviewing at least some of

---

"state a claim to relief that is plausible on its face," *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 570). Construing, as we must, all well-pleaded facts in the light most favorable to Wikimedia, *SD3*, 801 F.3d at 422, Wikimedia's claim that its "communications almost certainly traverse" every chokepoint is enough to satisfy the plausibility requirement. J.A. 48.

Wikimedia's communications. To put it simply, Wikimedia has plausibly alleged that its communications travel all of the roads that a communication can take, and that the NSA seizes all of the communications along at least one of those roads.

Thus, at least at this stage of the litigation, Wikimedia has standing to sue for a violation of the Fourth Amendment. And, because Wikimedia has self-censored its speech and sometimes forgone electronic communications in response to Upstream surveillance, it also has standing to sue for a violation of the First Amendment. *See Am. Civil Liberties Union*, 785 F.3d at 802 (holding that complaint established standing to assert First Amendment violation in addition to Fourth Amendment violation because "[w]hen the government collects appellants' metadata, appellants' members' interests in keeping their associations and contacts private are implicated, and any potential 'chilling effect' is created at that point"); *see also Cooksey v. Futrell*, 721 F.3d 226, 235 (4th Cir. 2013) ("In First Amendment cases, the injury-in-fact element is commonly satisfied by a sufficient showing of self-censorship, which occurs when a claimant is chilled from exercising his right to free expression.") (quotation marks and alteration omitted).

2.

The government resists this conclusion, asserting that the Wikimedia Allegation "rest[s] on speculation as to the scope and scale of Upstream collection, and the means by which that collection is accomplished." Appellees' Br. at 23. The district court said much the same, and the best way to address this contention is by examining the ways in which that court misapplied *Clapper*'s discussion of speculative injury.

Unlike in *Clapper*, where the plaintiffs based their theories of standing on prospective or threatened injury and actions taken in response thereto, Wikimedia pleaded an actual and ongoing injury, which renders *Clapper*'s certainly-impending analysis inapposite here. *Compare Schuchardt*, 839 F.3d at 351 (distinguishing *Clapper* and its discussion of a "speculative chain of possibilities" because plaintiff's "alleged [Fourth Amendment] injury has already occurred insofar as he claims the NSA seized his emails"), *with Beck*, 848 F.3d at 267–69, 274–75 (applying *Clapper*'s certainly impending standard to a motion to dismiss an action under the Privacy Act of 1974, and finding plaintiff's allegation that "her information 'will eventually be misused as a result of'" a data breach that compromised her personal information too speculative to establish standing).

In other words, the Wikimedia Allegation is different in kind than the facts (or lack thereof) alleged in *Clapper* to establish standing at summary judgment. That brings us to our next point. By relying so heavily on *Clapper*, the district court blurred the line between the distinct burdens for establishing standing at the motion-to-dismiss and summary-judgment stages of litigation. Put another way, what may perhaps be speculative at summary judgment can be plausible on a motion to dismiss.

For example, the district court characterized Wikimedia's allegations as "speculative" based upon its own observation that it's unclear whether the NSA is "using [its] surveillance equipment to its full potential" to intercept "all communications passing through" chokepoints upon which the NSA has installed surveillance equipment. J.A. 190, 198–99. That observation might be appropriate with the benefit of an evidentiary

record at summary judgment, but coming as it did on a motion to dismiss, it had the effect of rejecting Wikimedia's well-pleaded allegations and impermissibly injecting an evidentiary issue into a plausibility determination. *See Schuchardt*, 839 F.3d at 347–48 (citing *Twombly*, 550 U.S. at 556); *SDR*, 801 F.3d at 431.

The district court made the same mistake by speculating that "the fact that all NSA surveillance practices must survive FISC review . . . suggests that the NSA is not using its surveillance equipment to its full potential." J.A. 190–91. Wikimedia's reliance at the motion-to-dismiss stage on publicly disclosed information about Upstream surveillance, purported NSA documents, technical rules about how the Internet works, and its understanding of its own operations is not, as the district court put it, "precisely the sort of speculative reasoning foreclosed by" *Clapper*'s discussion of how much factual material is necessary to satisfy the certainly-impending prong of the injury-in-fact element of Article III standing at summary judgment. J.A. 192.[8]

That's not to say that all of Wikimedia's allegations as to injury are both plausible and actual or imminent. For example, the district court was right to take issue with Wikimedia's probability calculation, which "is incomplete and riddled with assumptions." J.A. 197. But we need not look further into that allegation's deficiencies, because Wikimedia doesn't need it to establish standing.

We also reject the government's argument that Wikimedia hasn't pleaded enough facts to establish injury flowing from its intercepted communications. To the contrary,

[8] Like the Third Circuit, we assume without deciding that a heightened pleading standard does not apply to national security cases.

Wikimedia's detailed allegations suffice to plausibly establish cognizable injuries under the First and Fourth Amendments. *See Rakas v. Illinois*, 439 U.S. 128, 140 (1978) (providing that the "definition of [Fourth Amendment] rights is more properly placed within the purview of substantive Fourth Amendment law than within that of standing"); *Cooksey*, 721 F.3d at 235 ("The leniency of First Amendment standing manifests itself most commonly in the doctrine's first element: injury-in-fact."). At this stage of the litigation, that is enough.

Finally, we decline the government's invitation to consider its evidence, including the two declarations, which it says "supports the district court's analysis and undermines plaintiffs' allegations about how they surmise Upstream surveillance operates." Appellees' Br. at 23. The district court treated the government's motion to dismiss as a facial challenge to the complaint and didn't consider the government's evidence. We will follow suit and not look beyond the complaint and documents incorporated by reference therein. *See Beck*, 848 F.3d at 270 (explaining the differences between facial and factual challenges to standing). The government is free to bring a factual challenge on remand, where the district court in the first instance may consider Wikimedia's argument—should it choose to raise it again—that the intertwined nature of the jurisdictional and merits questions precludes such a challenge.[9]

[9] We decline to decide whether Wikimedia has established third-party standing. Wikimedia may, of course, raise that argument on remand.

***

We now turn to the Dragnet Allegation, which is that the NSA is "intercepting, copying, and reviewing substantially all" text-based communications entering and leaving the United States. J.A. 46. The district court arrived at the correct conclusion as to whether this allegation establishes standing, but only by incorrectly analogizing to *Clapper*. As we explain below, the reason this allegation fails to establish standing is that it does not contain enough well-pleaded facts entitled to the presumption of truth.

C.

1.

The Dragnet and Wikimedia Allegations share much in common. Because each alleges the same particularized and ongoing cognizable injuries, our analysis of the injury-in-fact, traceability, and redressability elements of Article III standing with respect to the Wikimedia Allegation also applies here. But there's a key difference in the scope of the two allegations. In the Dragnet Allegation, Plaintiffs must plausibly establish that the NSA is intercepting "substantially all" text-based communications entering and leaving the United States, whereas it's sufficient for purposes of the Wikimedia Allegation to show that the NSA is conducting Upstream surveillance on a single backbone link. Because Plaintiffs don't assert enough facts about Upstream's operational scope to plausibly allege a dragnet, they have no Article III standing.

In support of a dragnet and in addition to the assertions in the Wikimedia Allegation, Plaintiffs allege the following: (1) "given the way the government has described Upstream surveillance," including that its "aim is to 'comprehensively' and

'reliably' obtain communications to, from, and about targets scattered around the world," the NSA "has a strong incentive to intercept communications at as many backbone chokepoints as possible," and indeed "must" be doing so "at many different backbone chokepoints," J.A. 49–50; (2) the technical rules governing online communications make this conclusion "especially true," J.A. 50; and (3) a *New York Times* article asserts that the NSA "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," J.A. 51.

We hold that these allegations, even when supplemented by the Wikimedia Allegation, including that the NSA is conducting Upstream surveillance on at least seven backbone links,[10] are insufficient to make plausible the claim that the NSA is intercepting "substantially all" text-based communications entering and leaving the United States.

To begin with, the *New York Times* article is effectively a recitation of the Dragnet Allegation, and as such we ascribe little significance to it. The dissent takes issue with our treatment of this article because—as it must—it predates the complaint. Our friend

[10] Plaintiffs also reference "another NSA document [which] states that, in support of *FAA* [(i.e., the FISA Amendments Act of 2008)] *surveillance*, the 'NSA has expended a significant amount of resources to create collection/processing capabilities at many of the chokepoints operated by U.S. providers.'" J.A. 51 (emphasis added). As Plaintiffs note, there are "at least two kinds of surveillance" under the Act—PRISM and Upstream. J.A. 40. Pointedly, and unlike in numerous other allegations throughout their complaint, including the immediately preceding one which references an "NSA slide illustrat[ing] the Upstream surveillance facilitated by just a single provider . . . at seven . . . chokepoints," J.A. 50, Plaintiffs decline to specify which type of surveillance the NSA document refers to. Accordingly, we accept this allegation as true, but give it little weight.

misses the point. The article makes a broad statement almost identical to the Dragnet Allegation. Under the dissent's view, one expansive allegation is enough to make plausible another almost-identical allegation. That is not the law.

Furthermore, we accept as true Plaintiffs' allegation about what the NSA is incentivized to do, but even so, that fact, without more, doesn't establish a dragnet. That leaves Plaintiffs with their allegation about what the NSA "must" be doing, a contention that lacks sufficient factual support to get "across the line from conceivable to plausible." *See Twombly*, 550 U.S. at 570.

A point of emphasis—we are not rejecting the allegation because it's phrased as an absolute. Indeed, we've already credited as true Plaintiffs' allegation that the NSA "must be copying and reviewing all the international text-based communications that travel across" backbone links which the NSA is surveilling. J.A. 48. We did so because Wikimedia applied the rules governing Internet communications to Upstream surveillance's stated purpose to arrive at a reasonable conclusion about the technical means through which Upstream functions on the backbone links which the NSA surveils. One ground for that conclusion's reasonableness is that given that the NSA is surveilling a link, the rules governing Internet communications necessarily affect, to some degree, the way it surveils that link.

By contrast, in the Dragnet allegation, Plaintiffs seek to use the theory governing Internet communications in conjunction with Upstream surveillance's stated purpose to arrive at an allegation about what the program's *operational scope* must be. But neither theory nor purpose says anything about what the NSA is doing from an operational

standpoint. While both are relevant factors, without more they can't establish a dragnet. In that sense, the facts alleged here are far different than those in *Schuchardt*, where the plaintiff plausibly pleaded a dragnet under PRISM surveillance by describing "the technical means through which PRISM" functions and by "confirming PRISM's operational scope and capabilities" through exhibits "replete with details." 839 F.3d at 349–50. Those exhibits included purported NSA slides which listed "company names and the dates they began cooperating with the" NSA and "confirm[ed] that . . . the scale of the data collected by PRISM is so vast that the Government [had] difficulty processing it according 'to the norms to which [it had] become accustomed.'" *Id.* at 350.

The last hope for the Dragnet Allegation, then, is to supplement the "must" allegation with facts detailing Upstream's operational scope. But even accepting the allegation that one telecommunications-service provider is facilitating Upstream surveillance at 7 of the approximately 49 chokepoints, we still don't think that Plaintiffs have plausibly alleged a dragnet. The allegations here fall short of the level of detail in *Schuchardt*, and were we to accept Plaintiffs' approach to standing, we would sanction the extrapolation of the plausible from the conceivable.

Our recent decision in *SD3* is not to the contrary. There, we considered the plausibility of a complaint alleging an antitrust conspiracy in violation of the Sherman Antitrust Act. 801 F.3d at 423. We explained that for such a "claim to survive . . . a plaintiff must plead parallel conduct *and* something 'more.'" *Id.* at 424 (quoting *Twombly*, 550 U.S. at 557)). "That more," we said, "must consist of further circumstances pointing toward a meeting of the minds." *Id.* (alteration and internal

quotation marks omitted). The plaintiff in *SD3* was able to establish that "more" by alleging the who, what, when, where, and why of a group boycott. *Id.* at 429–31.

Plaintiffs use our treatment of the "why" element in *SD3* to attach special significance to their allegation that the NSA has a strong incentive to establish a dragnet. But context is key. We observed in *SD3* that "motivation *for common action* is a key circumstantial fact." *Id.* at 431 (emphasis added) (alteration and internal quotation marks omitted). It should come as no surprise that motive is an important factor when establishing an antitrust conspiracy. *SD3* does not, however, stand for the broad proposition that motivation is always of special significance in plausibly pleading an injury.

Relatedly, the level of detail in the *SD3* complaint is of a different magnitude than the one here, and further supports our conclusion about the implausibility of the Dragnet Allegation. For example, the *SD3* plaintiff "identifie[d] the particular time, place, and manner in which the boycott initially formed" and gave "the means by which the defendants sealed their boycott agreement: a majority vote." *Id.* at 430. Those are the sorts of operational details, albeit in a case concerning a different subject matter, that are by and large absent here and which we think are vital to render plausible an allegation as sweeping as the one Plaintiffs posit. *See Twombly*, 550 U.S. at 558 ("[A] district court must retain the power to insist upon some specificity in pleading before allowing a potentially massive factual controversy to proceed."); *Swanson v. Citibank, N.A.*, 614 F.3d 400, 405 (7th Cir. 2010) ("A more complex case involving financial derivatives, or tax fraud that the parties tried hard to conceal, or antitrust violations, will require more

detail, both to give the opposing party notice of what the case is all about and to show how, in the plaintiff's mind at least, the dots should be connected.").

The dissent says that this analysis is flawed because the NSA's inability to predict a communication's path paired with its desire to "comprehensively acquire communications" renders plausible the allegation of a dragnet. The dissent thinks that's a "logical extension" of our crediting as true Wikimedia's allegation that the NSA reviews all communications that flow across each link that it surveils. Clearly, there are some similarities, in the sense that each allegation depends, in part, on the application of internet theory to a statement about Upstream's purpose. But, perhaps because it fails to grapple with any of the relevant case law, the dissent misses two subtle but key distinctions.

The allegation that we credit as true uses theory to explain how the NSA is doing something, given a defined operational scope. Moreover, that theory necessarily affects the way the NSA does what we know it to be doing. Conversely, the allegation that we do not credit as true uses theory to *define* scope. And, there's no direct link between that theory (the NSA doesn't know a communication's route) and operational scope. The dissent's analysis has no limiting principle and, if adopted, would dilute the plausibility pleading standard to a near-nullity.

In sum, Plaintiffs lack standing to sue for a violation of the Fourth Amendment under the Dragnet Allegation because they can't plausibly show that the NSA is intercepting their communications via a dragnet. From there, it follows that they also lack standing to sue for a violation of the First Amendment because "[a]llegations of a

subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm." *Clapper*, 133 S. Ct. at 1152 (alteration in original) (quoting *Laird v. Tatum*, 408 U.S. 1, 13–14 (1972)). Nor can Plaintiffs establish standing on the ground that Upstream surveillance compels them to take burdensome and costly measures. The Dragnet Allegation's implausibility leaves them with nothing more than "fears of hypothetical future harm," and they "cannot manufacture standing merely by inflicting harm on themselves based on" those fears. *Id.* at 1151.[11]

2.

Before concluding, we briefly address the dissent's contention that our analysis of the non-Wikimedia Plaintiffs' standing is superfluous.

Article III of the Constitution requires that we determine whether the non-Wikimedia Plaintiffs have standing because the complaint rests upon the premise that the NSA is seizing each Plaintiff's unique communications. As such, it includes the following request for individualized relief: "Order Defendants to purge all records of Plaintiffs' communications in their possession obtained pursuant to Upstream surveillance." J.A. 84. Thus, the Constitution requires that each Plaintiff be able to plausibly allege the Fourth Amendment injury in fact that the NSA has seized its communications, because if a Plaintiff cannot do so it doesn't have standing to, among

[11] We reach the same conclusion as to Joshua Dratel, who is a member of the National Association of Criminal Defense Lawyers. He too cannot show that his communications are being intercepted via a dragnet, and the district court correctly held that the claim that one of his clients "has received notice of [Section 702 surveillance]" didn't plausibly allege that the NSA targeted his client with Upstream surveillance. J.A. 68.

other things, seek an order requiring the NSA to purge its records. To hold otherwise would be to sanction a shortcut around "the irreducible constitutional minimum of standing." *Lujan*, 504 U.S. at 560.

Horne v. Flores, 557 U.S. 433 (2009), and *Village of Arlington Heights v. Metropolitan Housing Development Corp.*, 429 U.S. 252 (1977), are not to the contrary. Each case is quite different from ours, rendering inapplicable the standing-avoidance doctrine which the dissent reads them to embody.[12] Critically, in those cases each party for whom standing was at issue requested identical relief. *Horne*, 557 U.S. at 443; *Village of Arlington Heights*, 429 U.S. at 258. Thus, once the Court decided that a single party had standing, it made no difference to the resolution of either case whether any other party had standing. *See Horne*, 557 U.S. at 446 & n.2 (concluding that school superintendent had standing to seek vacatur of a district court's orders in their entirety and declining to consider whether state legislators also had standing to pursue identical relief); *Village of Arlington Heights*, 429 U.S. at 264 & n.9 (concluding that one individual plaintiff had standing to pursue declaratory and injunctive relief and declining to consider whether other individuals had standing to pursue identical relief); *see also, e.g.*, *Sec'y of the Interior v. California*, 464 U.S. 312, 319 n.3 (1984) ("Since the State of

[12] As for the dissent's invocation of then-Judge Roberts's notable quotable that "if it is not necessary to decide more, it is necessary not to decide more," context is key—that remark in a concurrence had nothing to do with standing, but rather pertained to the judge's disagreement with the majority's application of the *Chevron* doctrine. *See PDK Labs. Inc. v. Drug Enf't Admin.*, 362 F.3d 786, 799, 803–04 (D.C. Cir. 2004) (Roberts, J., concurring in part and concurring in the judgment). We don't disagree with the general sentiment. It's just not relevant here.

California clearly does have standing, we need not address the standing of the other respondents, whose position here is identical to the State's.").

Here, the Plaintiffs freely admit that they are not identical to one another. Instead, they fall into two different camps when it comes to demonstrating whether the NSA is seizing their communications. Moreover, the district court made an affirmative finding that none of the Plaintiffs had standing. Under these circumstances, we find it wholly appropriate (indeed necessary) to address fully this threshold question.

III.

For the reasons given, we vacate that portion of the district court's judgment dismissing the complaint as to Wikimedia and remand for proceedings consistent with this opinion. We otherwise affirm the judgment.

AFFIRMED IN PART,
VACATED IN PART,
AND REMANDED

DAVIS, Senior Circuit Judge, concurring in part and dissenting in part:

I agree with the holding that Wikimedia has standing to challenge the NSA's surveillance of its internet communications. However, because I would find that the non-Wikimedia Plaintiffs also have standing, I respectfully dissent in part.

I.

In order to explain my disagreement with the majority, I briefly recount the relevant allegations in this case, taken as true, of course, at this stage of the proceedings. Plaintiffs make essentially two sets of factual allegations: the first explaining how international internet communications function and the second describing how the NSA surveils international internet communications as they enter and exit the United States.

First, Plaintiffs allege that internet communications are governed by certain technical rules as they travel from sender to recipient. The majority of international internet communications that move through the United States are transmitted through forty-nine submarine cables and a limited number of terrestrial cables. These cables (combined with the cables and networks that transmit domestic internet communications) are known as the internet backbone, and the different physical entry and exit points into the United States are known as backbone links. The junctions where these cables meet are chokepoints through which nearly all international internet traffic passes. Internet communications do not flow along the backbone as discrete and intact entities but instead are broken into smaller packets of information. The packets that make up a single internet communication travel to their common destination independently from one another — in the process becoming intermingled with packets from unrelated

communications — and are reassembled only once they reach their destination. Each packet reaches its destination following a different and wholly unpredictable path, which is determined by rapidly changing factors such as network conditions. Because packets travel along independent and dynamic paths, communications sent between two individuals in "real-time" can traverse different backbone links "even though the end points are the same." J.A. 50. Similarly, a single individual's communications sent at different times can traverse different backbone links.

Second, based on the government's disclosures and media reports, Plaintiffs allege that the NSA is surveilling internet communications as they travel along the internet backbone, a practice known as Upstream surveillance. The NSA accomplishes this by installing surveillance devices at backbone links, which allow the agency to copy the internet communications traversing these links. The NSA searches the copied communications for selectors. Selectors are "specific communications facilit[ies]" (e.g. email address, telephone numbers, and IP addresses) associated with the NSA's foreign surveillance targets. PCLOB Report 32. The NSA retains communications sent to or from a selector as well as communications containing a selector in their content, which are known as "about communications." About communications are not necessarily sent to or from a foreign surveillance target. According to the government's disclosures, surveillance of about communications is necessary because the NSA seeks to "comprehensively acquire communications that are sent to or from its targets." *Id.* at 10. With respect to the scope of Upstream surveillance, the New York Times reported that, through the use of this form of surveillance, the NSA is copying "what is apparently most

e-mails and other text-based communications that cross the border." J.A. 51. Plaintiffs also quote an NSA document that states the "NSA has expended a significant amount of resources to create collection/processing capabilities at many of the chokepoints operated by U.S. providers through which international communications enter and leave the United States." *Id.*

II.

I agree with the majority's analysis concluding that *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013), does not control this case and that — accepted as true, as they must be — Plaintiffs' allegations satisfy the three elements of standing. The majority also correctly finds that the factual allegations necessary to establish Wikimedia's standing are plausible. However, the majority errs, both by reaching out to decide the issue of the non-Wikimedia Plaintiffs' standing[1] and, as well,

[1] *See Horne v. Flores*, 557 U.S. 433, 446 (2009) ("Because the Superintendent clearly has standing to challenge the lower courts' decisions, we need not consider whether the legislators also have standing to do so."); *Vill. of Arlington Heights v. Metro. Hous. Dev. Corp.*, 429 U.S. 252, 264 and n.9 (1977) (holding because "one individual plaintiff . . . has demonstrated standing," the Court "need not consider whether the other individual and corporate plaintiffs have standing to maintain the suit"). The majority's "same relief" gloss on *Horne* and *Arlington Heights* completely reads out of Justice Alito's opinion in *Horne* the following sentence: "[I]n *all standing inquiries*, the critical question is whether *at least one petitioner* has alleged such a personal stake in the outcome of the controversy as to warrant his invocation of federal-court jurisdiction." *Horne*, 557 U.S. at 445 (citations and internal quotation marks omitted). In any event, this case actually fits within the majority's "same relief" paradigm because all plaintiffs seek declaratory and injunctive relief intended to shut down the government's Upstream surveillance program. The mere fact that a "purging order" of the sort contemplated by the majority would operate only to "purge" seized communications of a particular plaintiff is a thin reed indeed on which to base the majority's unnecessary door-closing result.
(Continued)

in the answer it gives to the question it need not even reach in holding that the non-Wikimedia Plaintiffs' lack standing because the pertinent allegations are not plausible.

In order to find that Wikimedia has standing in this action, the majority credits as true three factual allegations. *First*, because Wikimedia sends and receives so many international internet communications, its communications travel across every internet backbone link. *Second*, based on the government's disclosures, the NSA is surveilling at least one backbone link. *Third*, the NSA intercepts and copies every packet that passes through the backbone link(s) being surveilled (what the majority calls the Wikimedia Allegation). The third allegation is not based on Plaintiffs' knowledge of the NSA's surveillance techniques. Instead, the majority finds this factual allegation is plausible

---

It is not clear to me why the majority elects to ignore the Chief Justice's sage admonition: "[I]f it is not necessary to decide more, it is necessary not to decide more." *PDK Labs., Inc. v. Drug Enforcement Admin.*, 362 F.3d 786, 799 (D.C. Cir. 2004) (Roberts, J., concurring in part and concurring in the judgment). The majority's assertion to the contrary notwithstanding, I think I know *dicta* when I see it, and here I see *dicta*. If, in fact, the Wikimedia Plaintiffs go on to prove their claims in this case, i.e., establish a violation of the Fourth Amendment as to *themselves*, it is beyond my capacity to conjure a rational basis on which the non-Wikimedia Plaintiffs would not be entitled to similar relief from seizures effected pursuant to the Upstream program and of course, the dismissal here of the non-Wikimedia Plaintiffs will be without prejudice. *S. Walk at Broadlands Homeowner's Ass'n v. OpenBand at Broadlands, LLC*, 713 F.3d 175, 185 (4th Cir. 2013).

In sum, the day cannot be far off when defendants in a broad array of multi-plaintiff cases will point to the majority's holding in this case as authority requiring already short-handed and overworked federal district judges to separately assess the standing of each and every plaintiff in complex, impact litigation. Needless to say, we should avoid imposing such a requirement in the absence of the absolute necessity that we do so.

because it is based on Upstream surveillance's stated purpose and the technical rules that govern internet communications. The logical chain is as follows: The NSA has acknowledged that it uses Upstream surveillance to target "about communications," which contain a selector in the content of the communication. Before it can search the contents of an internet communication that has been broken up into discrete packets while in transit, the NSA must copy and reassemble all of the packets that make up the communication. However, packets from targeted communications cannot be segregated from the packets of unrelated communications. Thus, in order to "reliably" intercept targeted communications, the NSA must copy all of the packets that flow across a backbone link so that the government can be assured that it has captured all of the packets that make up the targeted communication (and in the process capturing unrelated packets). J.A. 48–49.

Conversely, under the majority's "crabbed plausibility analysis," *see Woods v. City of Greensboro*, --- F.3d ---, ---, 2017 WL 1754898, *2 (4th Cir. 2017), the non-Wikimedia Plaintiffs are denied standing because, in the majority's view, those Plaintiffs rely on an implausible guess regarding Upstream surveillance's operational scope. For the non-Wikimedia Plaintiffs to have standing, according to the majority, Plaintiffs must plausibly allege an additional fact beyond those discussed with respect to Wikimedia: the NSA is surveilling most backbone links (what the majority calls the Dragnet Allegation). Just as with the Wikimedia Allegation, Plaintiffs base this factual allegation on Upstream

surveillance's stated purpose and the technical rules governing internet communications.[2] However, the majority finds this allegation implausible because it believes that "neither theory nor purpose says anything about what the NSA is doing from an operational standpoint." Op. at 33. This misapprehends the full scope of Plaintiffs' allegations.

Plaintiffs have plausibly alleged that the NSA surveils most backbone links because — based on the technical rules governing internet communications — the agency cannot know which link the communications it targets will traverse when they enter or leave the United States. The path that packets take along the internet backbone is determined dynamically based on unpredictable conditions. Thus, a communication sent by a surveillance target can enter the United States through one backbone link, but an immediate response returned to the surveillance target can traverse a different backbone link. Similarly, communications sent by a surveillance target at different times or locations can traverse different backbone links. Given this technical limitation, the government's disclosure that the NSA seeks to "comprehensively acquire communications that are sent to or from its targets," J.A. 49, renders Plaintiffs' allegation plausible. If the NSA cannot know which backbone link its targets' internet

[2] Plaintiffs provide additional support for this allegation by corroborating it with a N.Y. Times report, which stated that the NSA is surveilling "most e-mails and other text-based communications that cross the border." J.A. 51. The majority finds that this report is entitled to "little significance" because it "is effectively a recitation of" Plaintiffs' allegation. Op. at 32. The N.Y. Times report predates the complaint, however; thus, the allegation is a "recitation" of the factual news report, not the other way around. Moreover, the fact that Plaintiffs based their allegation on factual news reporting rather than their own conjecture means the allegation is entitled to more weight not less.

communications will traverse, then the only way it can comprehensively acquire its targets' communications is by surveilling virtually every backbone link.

This allegation is essentially a logical extension of Plaintiffs' earlier allegation that the NSA must copy every communication that flows across a backbone link it surveils. Just as it is plausible that the government must copy all of the packets that flow through a backbone link in order to "reliably" capture the packets that make up a targeted internet communication, because the government does not know across which backbone link a communication will travel, it is also plausible that the government must monitor virtually every link in order to "comprehensively" capture its targets' communications. Given that we review here a motion to dismiss and not a motion for summary judgment, the non-Wikimedia Plaintiffs have provided enough factual support to their allegation to survive dismissal.

III.

For the reasons set forth, while I discern no need whatsoever to review the district court's legal determination of the non-Wikimedia Plaintiffs' standing, I respectfully dissent from the majority opinion's unnecessary resolution of that issue.