No. 20-1191

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

WIKIMEDIA FOUNDATION,

Plaintiff-Appellant,

v.

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE; PAUL M. NAKASONE, 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; JOHN L. RATCLIFFE, in his official capacity as Director of National Intelligence; DEPARTMENT OF JUSTICE; and WILLIAM P. BARR, in his official capacity as Attorney General,

Defendants-Appellees.

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

BRIEF FOR APPELLEES

ETHAN P. DAVIS
Acting Assistant Attorney General

H. THOMAS BYRON III
JOSEPH F. BUSA
Attorneys, Appellate Staff
Civil Division, Room 7537
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530
(202) 305-1754

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Cases: **Page(s)**

Statutes:

Rule:

Legislative Materials:

Other Authority:

INTRODUCTION

Plaintiff seeks to challenge the legality of a certain type of foreign-intelligence surveillance, called Upstream, conducted by the National Security Agency (NSA) under statutory and court authorization. To maintain this suit, plaintiff must support its theory of standing with evidence that a reasonable fact-finder could use to conclude that NSA actually does, as plaintiff asserts, copy its communications. As the district court held, plaintiff has not met that burden.

The government invoked the state-secrets privilege over highly classified information, including where and how Upstream surveillance is conducted and whether it involves copying plaintiff's communications. The district court upheld the privilege, and, on appeal, plaintiff does not challenge the court's conclusion that disclosure of the privileged information would gravely damage national security. Accordingly, under this Court's case law, that privileged information cannot be used by either party or the court. The court thus correctly denied discovery of privileged information. And the court also correctly held that dismissal was required because any further litigation would threaten to disclose state secrets. Plaintiff seeks to avoid these straightforward consequences of the state-secrets privilege by purporting to discover what it says is an implicit loophole buried in the third clause of the sixth paragraph of a 40-year-old statute, 50 U.S.C. § 1806(f). But that statute has no application here and does not silently displace the privilege. Nor does any publicly available evidence support plaintiff's theory of standing.

STATEMENT OF JURISDICTION

Plaintiff invoked the district court's jurisdiction under 28 U.S.C. § 1331. JA 40. Final judgment was entered on December 17, 2019. JA 33. Plaintiff filed a timely notice of appeal on February 14, 2020. JA 4124. This Court has jurisdiction under 28 U.S.C. § 1291.

STATEMENT OF THE ISSUES

The questions presented are:

1. Whether the district court correctly held that 50 U.S.C. § 1806(f) does not permit plaintiff to learn state secrets about the methods and subjects of foreign-intelligence surveillance or require *in camera* review of such secrets in the circumstances of this case;

2. Whether the district court correctly held that plaintiff identified no admissible evidence that NSA had chosen to conduct Upstream surveillance in a manner that would result in Wikimedia's communications actually being copied; and

3. Whether the district court correctly held that the state-secrets privilege required dismissal because further adjudication would threaten to disclose state secrets.

PERTINENT STATUTES AND REGULATIONS

Pertinent statutes and regulations are reproduced in the addendum to this brief.

STATEMENT OF THE CASE

A. Factual and Legal Background

1. Upstream surveillance under Section 702 of the Foreign Intelligence Surveillance Act

In this lawsuit, plaintiff attempts to challenge the legality of targeted electronic surveillance conducted by NSA under Section 702 of the Foreign Intelligence Surveillance Act (FISA). That provision of FISA creates a court-authorized mechanism whereby the government may "target[] … persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a). Such surveillance is limited in important ways. The government "may not intentionally target any person known at the time of acquisition to be located in the United States" or "a United States person reasonably believed to be located outside the United States." *Id.* § 1881a(b)(1), (3). And Section 702 surveillance "shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States." *Id.* § 1881a(b)(6). A specialized Article III court—the Foreign Intelligence Surveillance Court (FISC)—supervises Section 702 surveillance and ensures compliance with these limitations. *Id.* § 1881a(j).

The Privacy and Civil Liberties Oversight Board (PCLOB), an independent government agency, 42 U.S.C. § 2000ee(a), has described two known types of Section 702 surveillance: PRISM and Upstream. Plaintiff seeks to challenge Upstream, so called because it "occurs 'upstream' in the flow of communications between

communication service providers" with the "compelled assistance … of the providers that control the telecommunications backbone over which communications transit." JA 2474 (PCLOB report).

Upstream surveillance occurs with regard to a specific, tasked electronic communication "selector," JA 178 n.2 (Coats decl.), such as, hypothetically, an email address. The government identifies a selector used by a non-U.S. person abroad, and determines that collection of communications to or from that selector is likely to yield foreign-intelligence information. *Id.* at 177-78 & n.2. Identified selectors are then "sent to a United States electronic communication service provider to acquire communications that are transiting through circuits that are used to facilitate [i]nternet communications, what is referred to as the '[i]nternet backbone.'" JA 2475-76 (PCLOB report).

"[I]n the course of the Upstream collection process, certain [i]nternet transactions transiting the [i]nternet backbone network(s) of certain electronic communication service provider(s) are filtered for the purpose of excluding wholly domestic communications and are then scanned to identify for acquisition those transactions that are to or from … persons targeted in accordance with the applicable NSA targeting procedures; only those transactions that pass through both the filtering and the scanning are ingested into Government databases." JA 177-78 (Coats decl.) (footnote omitted). Though the government has disclosed this general description of Upstream, "operational details … remain highly classified." JA 178.

2. The state-secrets privilege

Under the state-secrets privilege, certain sensitive national-security information is privileged and absolutely protected from disclosure in litigation. "[T]he United States may prevent the disclosure of information in a judicial proceeding if there is a reasonable danger that such disclosure will expose military [or state-secret] matters which, in the interest of national security, should not be divulged." *El-Masri v. United States*, 479 F.3d 296, 302 (4th Cir. 2007) (quotation marks omitted).

Evaluating a claim of privilege involves three steps. First, the "head of the department which has control over the matter" must make a "formal claim of privilege … after actual personal consideration by that officer." *El-Masri*, 479 F.3d at 304. Second, the court determines whether there is a "reasonable danger that its disclosure will expose military (or diplomatic or intelligence) matters which, in the interest of national security, should not be divulged." *Id.* at 305, 307. If the court determines that the information is privileged, it is "remove[d] … from the proceedings entirely." *Id.* at 306. Third, the court evaluates the effect of the successful privilege claim on the litigation. The proceeding "must be dismissed if the circumstances make clear that privileged information will be so central to the litigation that any attempt to proceed will threaten that information's disclosure." *Id.* at 308.

B. Prior Proceedings

Plaintiff Wikimedia Foundation operates Wikipedia, "one of the top ten most-visited websites in the world." JA 62 (am. compl.). In 2015, plaintiff and eight other

organizations brought this civil suit against the government, seeking an injunction against Upstream surveillance. JA 39, 93.

1. Dismissal and appeal

The district court initially dismissed the complaint for lack of standing. *Wikimedia Found. v. NSA*, 143 F. Supp. 3d 344 (D. Md. 2015). In the first appeal, this Court affirmed with respect to all eight other plaintiffs but reversed with respect to Wikimedia. *Wikimedia Found. v. NSA*, 857 F.3d 193 (4th Cir. 2017). Plaintiffs raised two theories of standing: a "Dragnet Allegation," contending that NSA is "intercepting, copying, and reviewing substantially all" internet "communications entering and leaving the United States," and a "Wikimedia Allegation" contending that, even if not a dragnet, Upstream would copy at least some Wikimedia communications. *Id.* at 202. Wikimedia's theory rested on three allegations: (i) Wikimedia's "communications almost certainly traverse every international backbone link connecting the United States with the rest of the world," (ii) the government was allegedly monitoring at least one such link, and (iii) wherever the government conducts Upstream surveillance, it must be copying *everything* transiting the link due to "the technical rules of how the [i]nternet works," *id.* at 204, 210. No other method, plaintiff maintained, was technologically possible.

This Court held that all three elements of Wikimedia's theory were plausibly pled—"at least at this stage of the litigation" in which evidence was not yet required. 857 F.3d at 211. By contrast, this Court affirmed dismissal of the other eight

plaintiffs for lack of standing because the Dragnet Allegation was unsupported by well-pleaded facts. *Id.* at 213-16. An "allegation about what the NSA 'must' be doing" based on NSA's asserted incentives "lacks sufficient factual support to get 'across the line from conceivable to plausible.'" *Id.* at 214.

2. Remand, state secrets, and summary judgment

a. On remand, plaintiff sought jurisdictional discovery on its theory of standing. The government invoked the state-secrets privilege by filing the declaration of Daniel Coats, then the Director of National Intelligence. JA 171-89. Coats explained that he was the head of the Intelligence Community and the official who controlled the relevant information. JA 172-73. After personal consideration of the matter, JA 178, Coats attested that the state secrets at issue "must be protected" because their "disclosure reasonably could be expected to cause serious damage, and in many cases exceptionally grave damage, to the national security of the United States," JA 174. The privilege covered, among other things, whether anyone's communications "have been subject to Upstream," "technical details concerning the methods, processes, and devices" involved, and "any specific location(s)" where Upstream surveillance occurs. JA 179-80.

As Coats explained, disclosure of this information would cause serious and, in many cases, exceptionally grave damage to national security. "If the Government were to reveal that an individual or entity is" the "subject of intelligence-gathering," that surveillance capability "would certainly be compromised." JA 182. "On the

other hand, if the Government were to reveal that an individual or entity is not" the "subject of intelligence-gathering," adversaries could avoid surveillance. *Id.* Disclosing how Upstream surveillance occurs "would reveal to our adversaries the extent of the ability of the United States to monitor and track their activities," thereby "helping our adversaries evade detection." JA 184. Disclosing the location(s) where surveillance occurs "would assist foreign adversaries in trying to evade particular channels of communications that are being monitored, exploit any particular channels of communications that are not being monitored, and target [such] location(s)" for "hostile action." JA 185.

These national-security harms were described in greater detail by then-Deputy Director of the National Security Agency, George Barnes, in a classified declaration. JA 199; JA 202-69 (redacted version). That classified declaration is available for this Court's review by request to the Classified Information Security Officer.

b. The court upheld the state-secrets privilege. JA 689-715. The government satisfied the procedural prerequisites by filing the declarations described above. JA 711-12. And the court determined that the information was, in fact, privileged because its release could be expected to harm national security by "undermin[ing] ongoing intelligence operations, depriv[ing] the NSA of existing intelligence methods," and helping "foreign adversaries" to "evade U.S. intelligence operations and to conduct their own operations against the United States." JA 712-13. The court thus denied plaintiff's motion to discover state secrets. JA 715.

The court also rejected plaintiff's contention that, notwithstanding the state-secrets privilege, the court nonetheless must decide standing and the merits of plaintiff's case by reviewing privileged materials *in camera*. JA 697-708. Plaintiff contended that an *in camera* review provision in FISA, 50 U.S.C. § 1806(f), applied here and displaced the privilege. JA 697. The court held that Section 1806(f) did not apply "where, as here, a plaintiff has not yet established that it has been the subject of electronic surveillance." JA 698.

c. The government then sought summary judgment, which the court granted on two independent grounds. The court concluded that, even if Wikimedia's communications transit every internet backbone link between the United States and the rest of the world, and even if the government were thought to conduct Upstream surveillance on at least one such link, plaintiff failed to identify evidence that the government copies all communications that travel across a monitored link. JA 4090-4105. It was undisputed that Upstream surveillance could be conducted in at least *two* technically feasible ways, one of which would filter for communications of likely intelligence value *before* copying. JA 4084. Because plaintiff identified no admissible evidence that the government chose to use a method that would result in copying Wikimedia's communications, rather than one that would not, the court granted summary judgment to the government. JA 4095-4105. The court also held that state

secrets regarding Upstream are so central to the case that further adjudication would threaten national security, and dismissal was required. JA 4105-11.

SUMMARY OF ARGUMENT

I. The district court correctly denied discovery into state secrets. Plaintiff sought highly classified information about Upstream, including how and where surveillance is conducted. The court correctly upheld the state-secrets privilege over such information. Applying this Court's case law, the court correctly concluded that privileged information must be removed from the case entirely, and the court denied the motion to compel disclosure of privileged information.

Plaintiff's only argument for reversal of that order is its mistaken contention that an inapposite procedure for *in camera* review established under FISA, 50 U.S.C. § 1806(f), applies here and silently displaces the state-secrets privilege. Section 1806(f) is a shield the government can invoke when it seeks to use information obtained or derived from electronic surveillance against an aggrieved person in litigation. Before allowing use of the information, a court considers the legality of the surveillance *in camera* to determine whether the information may be used or must be suppressed. That procedure does not apply here because the government does not seek to use information obtained or derived from electronic surveillance against plaintiff. And nothing in Section 1806(f) indicates Congress's intent—first discovered

40 years after that provision was enacted—to displace the longstanding and constitutionally grounded privilege.

II. The district court also correctly granted summary judgment. From the outset, plaintiff has staked its standing on three allegations: (i) its communications transit every international internet link, (ii) the government conducts surveillance on at least one such link, and, (iii) wherever the government conducts surveillance, it must copy all communications because of what plaintiff describes as the technical rules governing the internet. Plaintiff has identified no admissible evidence regarding the second allegation, and this Court can affirm on that basis alone. Plaintiff has also abandoned its third (mistaken) allegation that there is only one technical means of conducting surveillance. Plaintiff now asserts that, as between at least two technically feasible methods of conducting surveillance, the government has chosen a method that results in copying its communications as opposed to one that does not. But plaintiff has identified no evidence supporting that theory, which rests entirely on speculation about NSA's priorities and mission requirements—matters known only to NSA, and well outside the knowledge and expertise of plaintiff's internet expert.

III. In any event, dismissal is independently required because further adjudication would reveal state secrets. It is undisputed that the location(s) and technical means by which Upstream surveillance occurs, and the identities of persons subject to Upstream surveillance, are state secrets. And those issues are central to

standing. Virtually any response the government might make to plaintiff's allegations would threaten to disclose state secrets, as would any effort by plaintiff to identify facts concerning its theory of standing. The district court thus correctly held that dismissal is required on this independent ground.

STANDARD OF REVIEW

This Court reviews de novo a district court's grant of summary judgment, *CTB, Inc. v. Hog Slat, Inc.*, 954 F.3d 647, 658 (4th Cir. 2020), as well as its "legal determinations involving state secrets," *El-Masri*, 479 F.3d at 302.

ARGUMENT

I. The District Court Correctly Upheld the State-Secrets Privilege and Denied Discovery.

A. Information Subject to the State-Secrets Privilege Cannot Be Used in This Case.

In *United States v. Reynolds*, 345 U.S. 1 (1953), the Supreme Court recognized the state-secrets privilege as a longstanding feature of our legal system and applied it to deny plaintiffs discovery into privileged material, the disclosure of which would threaten national security. Since then, this Court has developed a robust body of case law applying the privilege in diverse circumstances and uniformly holding that, where the privilege is properly invoked, plaintiffs may not compel discovery into privileged material. *E.g.*, *Abilt v. CIA*, 848 F.3d 305 (4th Cir. 2017); *El-Masri*, 479 F.3d at 304; *Sterling v. Tenet*, 416 F.3d 338 (4th Cir. 2005).

Those longstanding precedents resolve this case. The government invoked the state-secrets privilege over, among other things, highly classified information regarding the location(s) and technical means by which Upstream surveillance is conducted—information plaintiff sought in jurisdictional discovery regarding standing. The district court properly applied this Court's precedents, upheld the privilege, removed the privileged information from this case completely, and denied plaintiff's motion to compel discovery into privileged matters. JA 709-15.

The court first held (JA 711), as a procedural matter, that the then-Director of National Intelligence, the "head of the department which has control over the matter," made a "formal claim of privilege" after "actual personal consideration." *El-Masri*, 479 F.3d at 304. The court then correctly held, as a substantive matter, that the information at issue is a state secret because disclosure "would undermine ongoing intelligence operations, deprive the NSA of existing intelligence methods," and help "foreign adversaries" to "evade U.S. intelligence operations" and "conduct their own operations against the United States." JA 712-13; *Sterling*, 416 F.3d at 346 ("[I]ntelligence-gathering methods or capabilities" fall "within the definition of state secrets."). Even the existence or nonexistence of "surveillance of an organization such as plaintiff" is a state secret because it "would provide insight into the structure and operations of the Upstream surveillance program" and "undermine [its] effectiveness." JA 714.

In this appeal, plaintiff does not dispute the procedural sufficiency of the government's assertion of the privilege, nor does plaintiff dispute the harm to national security that would result from disclosure of the privileged information.[1] Accordingly, the district court properly upheld the privilege.

The consequence under this Court's case law is clear: The state-secrets privilege precludes plaintiff's efforts to force the government to disclose the details of highly classified national-security information about foreign-intelligence surveillance. Information subject to the state-secrets privilege is "absolutely protected from disclosure—even for the purpose of in camera examination by the court." *El-Masri*, 479 F.3d at 306. Privileged information is "remove[d] … from the proceedings entirely." *Id.* Once the privilege is properly invoked, a court is "neither authorized nor qualified to inquire further" into privileged matters. *Sterling*, 416 F.3d at 349. Even "the most compelling necessity cannot overcome the claim of privilege if the court is ultimately satisfied that [state] secrets are at stake." *Abilt*, 848 F.3d at 313.

[1] Plaintiff does assert that the government cannot claim the privilege with respect to a narrow statement about "web activity" in a court filing. Br. 62 n.20. That argument, appearing in a short footnote, is forfeited. *United States v. Arbaugh*, 951 F.3d 167, 174 n.2 (4th Cir. 2020). Even if the argument were not forfeited, plaintiff's speculation about the meaning of "web activity" in that filing is no basis for challenging the court's thorough conclusion that the relevant information is privileged. *Alfred A. Knopf, Inc. v. Colby*, 509 F.2d 1362, 1370 (4th Cir. 1975). And in any event, as explained below in Part II.A.3.b.ii, nothing about the supposed meaning of "web activity" in that court filing supports standing.

Applying these precedents, the district court here correctly denied plaintiff's motion to compel disclosure of privileged information. JA 715.

B. FISA's *In Camera* Procedure Does Not Apply Here or Displace the Privilege.

Plaintiff nevertheless seeks to evade that straightforward application of this Court's precedents concerning the state-secrets privilege. Plaintiff points to an *in camera* procedure contained in FISA, 50 U.S.C. § 1806(f)—quoted in full at page A2 of the Addendum to this brief—and purports to find in that procedure an implicit loophole, discovered more than 40 years after FISA was enacted, allowing any plaintiff alleging unlawful surveillance to avoid this court's precedents regarding the state-secrets privilege and compel the government to disclose privileged information, and thereby damage national security. Br. 42-56.

Plaintiff's contention fails for three independent reasons: (1) FISA's *in camera* procedure, Section 1806(f), does not apply here because the government does not seek to use any information obtained or derived from electronic surveillance against plaintiff, and plaintiff does not seek to suppress any such use or to discover materials for the purpose of suppressing any such use. (2) In any event, Section 1806(f) applies only to determine the legality of surveillance in certain circumstances and is not available to plaintiff to determine the predicate factual question of whether it was subject to surveillance. And (3) Section 1806(f) does not displace the state-secrets

privilege. This Court may affirm the district court's order denying the motion to compel on the basis of any, or all, of these grounds.

1. Section 1806(f) is the government's shield, not plaintiff's sword.

The section of FISA that contains the *in camera* procedure that plaintiff points to, 50 U.S.C. § 1806, regulates how the government uses information obtained or derived from FISA electronic surveillance. Indeed, that is the title of the section: "Use of information." *Id.* And the paragraphs of that section preceding the *in camera* procedure in (f) all regulate how the government uses information obtained or derived from electronic surveillance. Paragraph (a) requires that such information "may be used" only in compliance with minimization procedures; (b) says such information "may only be used" with the advance authorization of the Attorney General; (c) and (d) require that, if the government seeks to "use" such information "against an aggrieved person" in a legal proceeding, the government must "notify the aggrieved person"; and (e) provides that an aggrieved person against whom such information is to be "used" may "move to suppress" such use "on the grounds that" it was "unlawfully acquired." *Id.*

The particular provision at issue in this case, paragraph (f) of Section 1806, creates *in camera* procedures by which a court may then determine whether the government can use information obtained or derived from electronic surveillance against an aggrieved person, or if such use must instead be suppressed because the

surveillance at issue was unlawful. It does so by providing that, if one of three predicate circumstances is present, then, "if" the Attorney General files an affidavit triggering the *in camera* procedure, the district court shall review the underlying applications, orders, and related materials *ex parte* and *in camera* to determine "the legality of the surveillance." 50 U.S.C. § 1806(f). If the court "determines that the surveillance was not lawfully authorized or conducted, it shall … suppress the evidence … or otherwise grant the motion." *Id.* § 1806(g).

Section 1806(f) does not apply here because none of the three predicate circumstances listed at the outset of that provision are met. By its terms, Section 1806(f) may apply: (i) when the government intends to use evidence obtained or derived from electronic surveillance in a legal proceeding under paragraphs (c) and (d); (ii) when an aggrieved person against whom such evidence would be used files a motion to suppress under (e); and (iii) "whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States" to "discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under [FISA]." 50 U.S.C. § 1806(f).

It is undisputed that circumstance (i) is absent here, as the government has not given notice of any intent to use information obtained or derived from electronic surveillance against plaintiff. JA 698. To the contrary, by asserting the state-secrets

privilege, the government has affirmatively precluded itself and plaintiff from using any such information. It is similarly undisputed that circumstance (ii) is absent, as plaintiff does not move to suppress the use of any information obtained or derived from electronic surveillance. *Id.*

And circumstance (iii), on which plaintiff relies, is also absent. Plaintiff argues (Br. 46) that, because it filed a motion to compel discovery regarding Upstream surveillance, that motion fits within circumstance (iii) as a "motion or request … pursuant to any other statute or rule" to "discover or obtain applications or orders or other materials relating to electronic surveillance." 50 U.S.C. § 1806(f). And plaintiff contends that this portion of FISA created plaintiff-friendly "discovery procedures." Br. 45.

But Section 1806(f) creates no discovery rights not already present under generally applicable law. The "motion or request" in circumstance (iii) is one made "pursuant to" whatever other valid rules or law may apply. 50 U.S.C. § 1806(f). Circumstance (iii) is thus not a free-floating right to discovery. It is a description of a situation in which certain motions, made pursuant to some *other* provision of law, may be removed by the government from adversarial adjudication in open court and submitted for *in camera* determination. In keeping with the rest of Section 1806 and paragraph (f), circumstance (iii) thus applies when the government seeks to use evidence obtained or derived from electronic surveillance against an aggrieved person

and the aggrieved person seeks to prevent such use. It serves as a backstop to circumstances (i) and (ii), ensuring that the aggrieved person against whom the evidence is to be used cannot prevent the government from invoking the government-protective procedures of Section 1806(f) for an *in camera* determination regarding whether such use is permitted by merely citing some *other* rule, besides the suppression motion and the notice provision discussed in the first two circumstances.

That conclusion follows from the text, title, and structure of Section 1806, in which all of the paragraphs preceding (f), and both circumstances preceding the third circumstance in paragraph (f), focus entirely on determining when and how the government may "use" information obtained or derived from electronic surveillance against an aggrieved person. Plaintiff misreads circumstance (iii)—buried in the middle of paragraph (f) in a section otherwise entirely about regulating the government's "use" of information—as making an abrupt right turn and serving a function completely unrelated to the rest of Section 1806. The statutory text does not support that implausible account. "If Congress indeed meant to make" Section 1806(f) what plaintiff says it is, "one would have expected a clearer indication of that intent." *Yates v. United States*, 574 U.S. 528, 540 (2015).

Instead, the text of circumstance (iii) confirms that it, too, like everything that surrounds it in Section 1806, governs when the government may use information obtained or derived from electronic surveillance. Where, as here, "general words

follow specific words in a statutory enumeration, the general words are construed to embrace only objects similar in nature to those objects enumerated by the preceding specific words." *Washington State Dep't of Soc. & Health Servs. v. Guardianship Estate of Keffeler*, 537 U.S. 371, 384-85 (2003). This interpretive principle "implies the addition of *similar* after the word *other*." Antonin Scalia & Bryan A. Garner, *Reading Law: The Interpretation of Legal Texts* 199 (2012). It thereby avoids "giving unintended breadth to the Acts of Congress." *Yates*, 574 U.S. at 543. Here, that principle ensures that circumstance (iii) covers a situation in which an aggrieved person creatively invokes a statute or rule *other* than the notice and suppression mechanisms in circumstances (i) and (ii) to achieve a *similar* effect.

Indeed, the legislative history "make[s] very clear" that circumstance (iii) does precisely that. S. Rep. No. 95-701, at 63 (1978). Section 1806(f)'s procedures "apply whatever the underlying rule or statute referred to in the motion," and Congress designed Section 1806(f) with this government-friendly backstop "to prevent the carefully drawn procedures in subsection ([f]) from being bypassed by the inventive litigant using a new statute, rule or judicial construction." *Id.* Section 1806(f) applies to "determine whether the surveillance" violated the legal "right[s] of the person *against whom the evidence is sought to be introduced*." *Id.* (emphasis added). The government may thus avoid application of Section 1806(f) by "choos[ing]" to "forgo the use of the surveillance-based evidence." *Id.* at 65; *see also* S. Rep. No. 95-604, at 57-58 (1977).

That Section 1806(f) serves that limited, government-protective function is also clear from Congress's choice of triggering mechanism. By its terms, Section 1806(f)'s *in camera* procedure applies only "*if* the Attorney General files an affidavit." 50 U.S.C. § 1806(f) (emphasis added). It is thus the government, not plaintiff, that "invoke[s]" and "trigger[s]" *in camera* proceedings. S. Rep. No. 95-701, at 63. Here, the government has not invoked Section 1806(f)'s government-protective *in camera* procedure because the government does not seek to use information obtained or derived from electronic surveillance against plaintiff, plaintiff has filed no motion calling any such use into question, and there is thus no need to resolve the question of whether such use would be permissible. Plaintiff's assertion that Section 1806(f) applies here ignores the plain text of the statute and assigns to itself a trigger that Congress left to the government.

Similarly illuminating is what happens after a court applies Section 1806(f)'s *in camera* procedure: the court determines the lawfulness of surveillance, and then the court uses that determination as the basis for either granting or denying a motion to suppress, or similar motion. 50 U.S.C. § 1806(g). The result of Section 1806(f) proceedings is thus not an award of final judgment on the merits, or even an adjudication of a motion for summary judgment, but a grant or denial of a specific type of motion for which the lawfulness of surveillance is the relevant rule of

decision. The district court could thus not, as plaintiff oddly suggests, use Section 1806(f) to review "any secret evidence bearing on standing or the merits." Br. 17.

Nor could the court decide plaintiff's motion to compel using Section 1806(f). The lawfulness of surveillance—the issue a court determines using Section 1806(f)—is the relevant metric for deciding whether to suppress evidence. And, where a motion for discovery is made to facilitate a party's attempt to suppress evidence, a court can decide whether to grant or deny suppression by evaluating the lawfulness of the surveillance *in camera* and thereby render discovery moot. But where, as here, a discovery motion has *nothing to do* with the government's use of information obtained or derived from electronic surveillance, or an attempt to prevent such use, a court cannot determine a litigant's entitlement to discovery by evaluating the lawfulness of surveillance. Plaintiff thus tries to fit a square peg in a round hole.

In sum, Section 1806(f) does not create discovery procedures benefiting those who litigate against the government. Plaintiff notes (Br. 45, 53-54) that Section 1806(f) can be employed in civil as well as criminal cases. *See United States v. Hamide*, 914 F.2d 1147, 1149 (9th Cir. 1990) (immigration). That merely confirms that, whether in a civil or criminal proceeding, if the government seeks to use information obtained or derived from electronic surveillance against an aggrieved person, the government may invoke the protections of Section 1806(f) to determine if such use is permitted or if the information must be suppressed. It does not follow, as plaintiff

mistakenly assumes, that FISA created an all-purpose discovery mechanism for plaintiffs who bring civil suits challenging the legality of alleged surveillance. Br. 53. As discussed above, nothing in the text, structure, or legislative history supports that view. To the contrary, Congress recognized that, if the government does not invoke Section 1806(f)'s *in camera* procedure, a litigant's motion would be determined under whatever other procedures might govern under generally applicable law. S. Rep. 95-701, at 63.

2. Even if plaintiff could invoke Section 1806(f), it would first have to show that it is an "aggrieved person."

a. Section 1806(f)'s *in camera* procedures apply only to determine the "legality" of electronic surveillance. 50 U.S.C. § 1806(f). Nothing in the text of the statute suggests that a court could use Section 1806(f) to help a plaintiff make the predicate *factual* showing of having been subject to surveillance.

Congress knows how to create a procedure to compel the government to "affirm or deny" whether a person was subject to certain types of surveillance. 18 U.S.C. § 3504(a)(1). The "affirm or deny" procedure that Congress *has* created has no application here. (Plaintiff does not contend otherwise. Indeed, plaintiff does not cite this provision at all.) And Section 1806(f) includes no similar language that could compel the government to tell plaintiff whether it has been subject to surveillance. This Court has previously compared the affirm-or-deny procedure in Section 3504 with Section 1806 in order to give meaning to important textual differences between

the two. *In re Grand Jury Subpoena (T-112)*, 597 F.3d 189, 198 (4th Cir. 2010). Applying the same approach here, the district court correctly concluded that Section 1806(f) applies "only after the individual has adduced evidence that he has been the [subject] of electronic surveillance." JA 700.

That conclusion is reinforced by Congress's definition of *whose* legal contentions may be resolved using Section 1806(f): an "aggrieved person." As the district court correctly concluded, "the text of § 1806(f)," by requiring that the relevant motion described in circumstance (iii) be made by an "aggrieved person," "makes clear that a party's status as an 'aggrieved person,' or the subject of surveillance, is a precondition to the application of § 1806(f)'s procedures." JA 699. Indeed, the statute defines an "[a]ggrieved person" as "a person who *is the target* of an electronic surveillance or any other person whose communications or activities *were subject* to electronic surveillance," 50 U.S.C. § 1801(k) (emphasis added)—not someone who merely *alleges* surveillance.

Moreover, as the district court noted, Section 1806's heading—"Use of information"—"suggests that Congress intended the provisions of § 1806," including the third circumstance in (f), "to apply where evidence already establishes the fact of surveillance, and the central dispute is instead how, and whether, information obtained via that electronic surveillance can be used." JA 702. The first two circumstances in which Section 1806(f) may apply involve "evidence that electronic

surveillance has occurred," JA 701—such as when the government provides notice or when an opposing party moves to suppress. 50 U.S.C. § 1806(c), (d) (notice); *id.* § 1806(e) (litigant may move to suppress once "aware of the grounds of the motion"). The district court thus correctly read the third circumstance, in which an "aggrieved person" files a motion, to similarly require, as a precondition, that the filer adduce evidence that it is aggrieved. *See Begay v. United States*, 553 U.S. 137, 142-43 (2008), *abrogated on other grounds by Johnson v. United States*, 135 S. Ct. 2551 (2015).

b. That is in keeping with Congress's desire to avoid requiring the government to make disclosures under Section 1806(f) that would damage national security. S. Rep. No. 95-701, at 65 (the government may "choose" to "forgo the use of the surveillance-based evidence" to avoid disclosures that "would damage the national security"). Plaintiff's reading of Section 1806(f), far from *avoiding* damaging disclosures, would *require* them. It would allow anyone to compel the government to disclose whether he or she has been subject to electronic surveillance merely by filing a complaint alleging that such surveillance has taken place. At that point, plaintiff says, it can force the government to submit, and the court to render a decision based on, state-secrets evidence regarding standing and aggrieved-person status. Br. 50.

The Supreme Court considered and rejected precisely that kind of procedure in *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013). There, as here, the plaintiffs failed to introduce sufficient evidence on summary judgment to support standing to

challenge surveillance. The Court rejected a suggestion "that the Government could help resolve the standing inquiry by disclosing to a court, perhaps through an *in camera* proceeding … whether it is intercepting [the plaintiffs'] communications." *Id.* at 412 n.4. Such a procedure "would allow a terrorist (or his attorney) to determine whether he is currently under U.S. surveillance simply by filing a lawsuit challenging the Government's surveillance program." *Id.* The court's "decision about whether to dismiss the suit for lack of standing would surely signal to the terrorist whether his name was on the list of surveillance targets." *Id.* The Court understandably rejected the invitation to create an *in camera* procedure with that kind of grave consequence for national security. It is thus unsurprising that Congress, too, declined to turn Section 1806(f) into a vehicle for forcing the government to confirm or deny highly classified operational details of NSA intelligence-gathering activities.

The D.C. Circuit, in analyzing this question, rejected the contention plaintiff raises here: "If the government is forced to admit or deny such allegations" of electronic surveillance, it "will have disclosed sensitive information that may compromise critical foreign intelligence activities." *ACLU Found. of S. Cal. v. Barr*, 952 F.2d 457, 468 & n.13 (D.C. Cir. 1991). The D.C. Circuit correctly interpreted Section 1806 as not creating a "duty to reveal ongoing foreign intelligence surveillance." *Id.* The court held that, in a summary judgment motion, "[t]he government would need only assert that plaintiffs do not have sufficient evidence to carry their burden of proving ongoing surveillance," and that, "[i]f plaintiffs are ultimately unable to come

forward with such evidence, the district court must conclude that there is no 'genuine' dispute about these material facts and enter summary judgment in favor of the government." *Id.* at 469. So, too, here.

The opinion of the Ninth Circuit in *Fazaga v. FBI*, -- F.3d ---, Nos. 12-56867, 12-56874, 13-55017, 2020 WL 4048696 (9th Cir. July 20, 2020), on which plaintiff relies, does not warrant a different outcome.[2] *Fazaga* held that dismissal on state-secrets grounds was premature. It incorrectly assumed that the government's invocation of the state-secrets privilege to *remove* information from the case indicated it might wish to *use* information obtained or derived from electronic surveillance against plaintiffs. *Id.* at *26. And it incorrectly treated the assertion of the privilege as if it invoked Section 1806(f). *Id.* Plaintiff makes neither argument here. *Fazaga* also held that Section 1806(f) silently displaces the state-secrets privilege. *Id.* at *22-*25. As explained below in Part I.B.3, this Court's precedents foreclose that conclusion.

In any event, as the district court here explained (JA 4113 & n.60), *Fazaga* indicated that a plaintiff would have to show that it is an aggrieved person for Section 1806(f) to apply. 2020 WL 4048696, at *9 (plaintiffs' allegations "are sufficient *if proven* to establish that [the plaintiffs] are 'aggrieved persons,'" (emphasis added)); *id.* at *41 & n.51 ("FISA-covered electronic surveillance [may] drop out of

[2] The government sought *en banc* rehearing in *Fazaga*, and ten judges dissented from denial of rehearing, explaining why the panel erred. 2020 WL 4048696, at *47-*58. A petition for a writ of certiorari would be due December 17, 2020.

consideration" on remand "if, for instance, [the plaintiffs] are unable to substantiate their factual allegations as to the occurrence of the surveillance."). Most tellingly, the *Fazaga* panel members also indicated that, in a circumstance where the use of Section 1806(f) procedures would itself lead to the disclosure of state secrets, the government would retain the option to seek dismissal to protect state secrets. *Id.* at *43 n.1. Here, as the district court correctly held, the existence or nonexistence of "surveillance of an organization such as plaintiff" is a state secret. JA 714. Accordingly, under *Fazaga*'s reasoning, the state-secrets privilege applies here.

c. Plaintiff attacks the distinction between determining the *legality* of surveillance and determining the *existence* of surveillance, and plaintiff insists that determining the latter "is simply the first step" in determining the former. Br. 54. But, again, Congress knows how to require the government to "affirm or deny" surveillance, 18 U.S.C. § 3504, and it has not done so here. Nor is it "illogical" to "bifurcate" standing and merits in cases like this. Br. 50-51. Indeed, that is the uniform basis on which challenges to alleged NSA surveillance have proceeded. *See, e.g.*, *Schuchardt v. President of United States*, 802 F. App'x 69, 74 (3d Cir. 2020). "[I]t is [*plaintiff's*] burden to prove [its] standing," not "the Government's burden to disprove standing by revealing details of its surveillance priorities." *Clapper*, 568 U.S. at 412 n.4. In seeking to force such disclosure here, it is plaintiff, and not the government, that seeks to bypass the "ordinary sequence of civil litigation." Br. 51.

Plaintiff asserts that "FISA was designed to permit civil claims to proceed by channeling discovery through Congress's chosen procedures." Br. 50. But nothing in Section 1806(f) purports to create a mandatory mechanism for resolving jurisdictional questions like standing in cases like this. And while, as plaintiff notes (Br. 44), the Church Committee hoped that "*the courts* w[ould] be able to fashion [*in camera*] discovery procedures … to allow plaintiffs with substantial claims to uncover enough factual material to argue their case," S. Rep. 94-755, at 337 (1976) (emphasis added), that does not change the fact that *Congress* created no such procedures. Congress, like the courts, decided *not* to create a system that would permit any person to file a complaint and thereby force the government to reveal whether the person's communications have been subject to surveillance. *Clapper*, 568 U.S. at 412 n.4.

Plaintiff worries that enforcing the statute's aggrieved-person requirement conflicts with what plaintiff asserts is Congress's "overriding purpose" of "ensur[ing] judicial review." Br. 51. But, as the district court noted (JA 4120), the Article III judges of the FISC already review the government's compliance with FISA and the Constitution. 50 U.S.C. § 1881a(a), (i), (j); JA 2849-55 (holding that Upstream complies with the Fourth Amendment). In light of this "comprehensive scheme" of court supervision, applying Congress's aggrieved-person requirement here "by no means insulates [Upstream] from judicial review." *Clapper*, 568 U.S. at 421.

Nor is the FISC the only court that hears challenges to the legality of surveillance. Individuals challenge the legality of surveillance when the government

uses information obtained or derived from electronic surveillance against an aggrieved person in a proceeding. 50 U.S.C. § 1806(c), (e). This Court frequently hears such challenges. *United States v. Dhirane*, 896 F.3d 295, 300 (4th Cir. 2018); *United States v. Hassan*, 742 F.3d 104, 138 (4th Cir. 2014); *United States v. Squillacote*, 221 F.3d 542, 553 (4th Cir. 2000). Recently, other courts of appeals have heard such challenges to the legality of surveillance under Section 702. *United States v. Hasbajrami*, 945 F.3d 641, 645 (2d Cir. 2019); *United States v. Mohamud*, 843 F.3d 420, 438 (9th Cir. 2016).

And, even absent use of information obtained or derived from electronic surveillance against an aggrieved person, civil plaintiffs could try to establish standing using non-privileged evidence, if—unlike here, see Part III below—standing could be litigated without unacceptable risk to national security. Plaintiff worries that applying the normal rules of discovery and the state-secrets privilege here would give the government the power to "unilaterally thwart judicial review of sweeping surveillance programs." Br. 16. But, as this Court has already explained, the government has no "unilateral" power over the state-secrets privilege, as a court considering the government's invocation of the privilege must carefully review and determine for itself that the information at issue is indeed properly protected by the privilege. *El-Masri*, 479 F.3d at 312. The district court did so here, and plaintiff offers no meaningful argument to the contrary.

Congress did not design Section 1806(f) to compel the government to disclose highly classified national-security information about the operation of foreign-

intelligence surveillance. That this is so does not, as plaintiff contends, "profoundly undermine the civil remedies that Congress enacted," Br. 52—remedies that plaintiff has not even invoked in this suit. Rather, it underscores the limits of what Congress did in providing for civil liability in FISA. 50 U.S.C. § 1810 (tying the civil liability of individual-capacity defendants to violations of the criminal prohibitions in Section 1809). That plaintiff wishes Congress had gone further than it did and provided for mandatory jurisdictional discovery *in camera* to facilitate suits like this, while mandating disclosure of classified information, does not make it so.

3. Section 1806(f) does not displace the state-secrets privilege.

Plaintiff seeks to invoke Section 1806(f) on the misguided notion that, if that provision were to apply, it would also silently displace the state-secrets privilege. That contention is irreconcilable with this Court's precedent making clear that the privilege has firm roots in the Constitution. Section 1806(f) says nothing about the privilege and does not purport to override it.

a. The state-secrets privilege is a long-standing and well-established feature of our legal system, with origins stretching back to early Anglo-American law. *Reynolds*, 345 U.S. at 6-9 & n.18 (citing, *inter alia*, the treason trial of Aaron Burr). By 1978, when FISA was enacted, "it [wa]s quite clear that the privilege to protect state secrets must head the list" of "the various privileges recognized in our courts." *Halkin v. Helms*, 598 F.2d 1, 7 (D.C. Cir. 1978).

This longstanding feature of our legal system enables the Executive Branch to fulfill its constitutional duties. As the Supreme Court has made clear, "[t]he authority to protect [national-security] information falls on the President as head of the Executive Branch and as Commander in Chief." *Department of Navy v. Egan*, 484 U.S. 518, 527 (1988) (citing *Totten v. United States*, 92 U.S. 105, 106 (1876), a case about the state-secrets privilege). And executive privileges that "relate[] to the effective discharge of a President's powers" are "constitutionally based." *United States v. Nixon*, 418 U.S. 683, 710-11 (1974). This Court has thus correctly recognized that the state-secrets privilege has "a firm foundation in the Constitution" and "performs a function of constitutional significance" because "it allows the executive branch to protect information whose secrecy is necessary to its military and foreign-affairs responsibilities." *El-Masri*, 479 F.3d at 303-04.

The separation of powers thus requires a clear statement by Congress before a court can conclude that a statute, such as FISA, displaces the privilege. As the Supreme Court has explained, "unless Congress *specifically* has provided otherwise, courts traditionally have been reluctant to intrude upon the authority of the Executive in military and national security affairs." *Egan*, 484 U.S. at 530 (emphasis added). Congress does not bring about a significant change in the Executive Branch's power to protect national security by happenstance, or by securing the President's approval of a bill with that unstated, yet startling, effect. *Cf. Franklin v. Massachusetts*, 505 U.S. 788, 800-01 (1992) (requiring, "[o]ut of respect for the separation of powers and the

unique constitutional position of the President," an "express statement by Congress" before concluding the Administrative Procedure Act applies to the President). Courts thus decline to interpret statutes as "significantly alter[ing] the balance between Congress and the President" or in a way that "raises 'serious' practical, political, and constitutional questions that warrant careful congressional and presidential consideration" without "affirmative evidence that these issues were considered in the legislative process and that Congress passed [the statute] with the understanding that it would" have those effects. *Armstrong v. Bush*, 924 F.2d 282, 289 (D.C. Cir. 1991).

There is no clear statement anywhere in FISA, much less Section 1806(f), indicating that Congress considered displacing the state-secrets privilege and intended to bring about such a stunning change in the Executive's authority to protect national-security information from compelled disclosure in litigation. Plaintiff does not contend otherwise.

b. Instead, plaintiff urges this Court to treat the state-secrets privilege as a run-of-the-mill creation of common law and to ask only whether Section 1806(f) "speaks directly," not to the continued existence of the privilege, but to protecting sensitive information. Br. 46-47. That inadequate inquiry gives short shrift to the constitutional roots and function of the privilege and risks upsetting a longstanding feature of the separation of powers without Congress having clearly considered whether to do so. But even under plaintiff's standard, there is no basis for concluding

that Congress displaced the state-secrets privilege. Nothing in FISA's text or legislative history addresses the privilege, either expressly or implicitly. Nor are Section 1806(f)'s government-protective features inconsistent with the government invoking the state-secrets privilege to prevent disclosure (even *in camera*) of classified information where necessary to protect national security.

The privilege and Section 1806(f) have different scopes and opposite functions. Far from "speaking to," and displacing, the privilege, FISA respects and complements it. Section 1806(f) applies when the government seeks to "use" information obtained or derived from electronic surveillance against an aggrieved person in legal proceedings, and Section 1806(f) provides a mechanism for adjudicating whether that information was lawfully obtained or instead must be suppressed. That is why it is the Attorney General (or his delegee)—the official responsible for government litigation—who triggers those statutory procedures. 50 U.S.C. §§ 1801(g), 1806(f). The state-secrets privilege addresses a different and broader concern: the government invokes the privilege to *remove* information from a case to protect national security from harms that would result from disclosure. That is why the "head of the department" responsible for the national-security information (often, as here, *not* the Attorney General) must "personal[ly]" (*not* through a delegee) make the privilege claim. *Reynolds*, 345 U.S. at 7-8. The privilege applies broadly, even in a case where the government is not a party. *Fitzgerald v. Penthouse Int'l, Ltd.*, 776 F.2d 1236 (4th Cir.

1985). And the privilege removes protected information from a case entirely, thus foreclosing even *in camera* proceedings. *Sterling*, 416 F.3d at 348.

Section 1806(f) does not establish its *in camera* procedure as the *exclusive* means for protecting national security. Indeed, even before FISA was enacted, courts "uniformly" used *in camera* procedures to determine the legality of foreign-intelligence surveillance in appropriate circumstances. *United States v. Belfield*, 692 F.2d 141, 149 (D.C. Cir. 1982). That such procedures comfortably coexisted with the privilege *before* FISA underscores that codification of *in camera* procedures for certain purposes *in* FISA does not displace the privilege. And Congress specifically intended to ensure that, even when Section 1806(f) could otherwise apply, the government would be able to "prevent[]" the court's "adjudication of legality" by simply "choos[ing]" to "forgo the use of the surveillance-based evidence" and thereby avoid risking that Section 1806(f)'s procedures "would damage the national security." S. Rep. No. 95-701, at 65. Plaintiff's displacement argument is inconsistent with that intent.

c. Plaintiff seems to argue (Br. 47) that Section 1806(f) should be read to displace the privilege because it applies "notwithstanding any other law." But that proviso applies only when one of the statute's three pre-requisite circumstances is met and only "if" the Attorney General files a particular affidavit. 50 U.S.C. § 1806(f). In that situation (which is not present here), then the court "shall" apply the procedures described in Section 1806(f), "notwithstanding any other law" that may provide for

other, public procedures to resolve the motion at issue. *Id.*; *see* S. Rep. No. 95-701, at 63 ("Although a number of different procedures might be used to attack the legality of the surveillance, it is this procedure 'notwithstanding any other law' that must be used to resolve the question."). Plaintiff would re-write the statute to provide that, "notwithstanding any other law" that the government may have at its disposal to protect the relevant information by removing it from a case, the Attorney General "shall" somehow be required to invoke Section 1806(f).

Plaintiff is on no firmer footing in asserting that "FISA's legislative history confirms Congress's preclusive intent." Br. 47. The particular portions of legislative history cited by plaintiff say nothing about displacing the state-secrets privilege. They instead address how Congress wanted to make FISA the exclusive means for conducting electronic surveillance for foreign-intelligence purposes.

Plaintiff is also mistaken in contending that separation-of-powers principles weigh in favor of displacing the privilege. Br. 48. To the contrary, applying a clear-statement rule protects the Executive's traditional powers regarding national security from encroachment by the legislature. A clear-statement rule would thus avoid a substantial question whether Congress may displace the privilege consistent with the separation of powers. As plaintiff notes, Congress has legislated regarding classified evidence in criminal prosecutions and congressional committees. Br. 49. That Congress has legislated in those arenas does not resolve the separate question whether Congress can deprive the Executive of the ability to safeguard national-security

information from compelled disclosure to the general public, in a circumstances where the government cannot avoid disclosure by declining to bring a prosecution. Courts are understandably "loath to conclude that Congress intended to press ahead into dangerous constitutional thickets in the absence of firm evidence that it courted those perils." *Public Citizen v. U.S. Dep't of Justice*, 491 U.S. 440, 466 (1989).

II. The District Court Correctly Granted Summary Judgment.

As a result of the state-secrets privilege, neither plaintiff nor the government could use privileged information to litigate standing. Plaintiff attempted to develop non-privileged evidence, relying primarily on the declarations of an expert. But, as the court correctly held, plaintiff failed to meet its burden on summary judgment of supporting standing with admissible evidence. JA 4091-4105.

Article III of the Constitution requires plaintiff to show, among other things, an "actual or imminent" injury. *Clapper*, 568 U.S. at 409. That requirement is "especially rigorous" where, as here, "reaching the merits" would force a court "to decide whether" Executive activities involving "intelligence gathering" are "unconstitutional." *Id.* at 408-09. Thus, plaintiff here must ultimately prove that the government copied its communications, or that, if the government has not done so yet, such copying is "certainly impending." *Id.* at 409.

As "[t]he party invoking federal jurisdiction," plaintiff has the "burden" of establishing standing "with the manner and degree of evidence required at the successive stages of the litigation." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561

(1992). When the government sought summary judgment, plaintiff thus had the burden of identifying evidence that a reasonable fact-finder could use to conclude that plaintiff's communications are copied. *CTB, Inc.*, 954 F.3d at 658. A "mere … scintilla of evidence" is insufficient, as is "[u]nsupported speculation." *Id.* at 658-59. Plaintiff must identify enough admissible evidence supporting its theory of standing that could warrant a standing determination in plaintiff's favor based on that evidence. *Id.*

Plaintiff has not done so.

A. Plaintiff Failed to Identify Evidence Supporting the Second and Third Elements of Its Theory of Standing.

Plaintiff's theory of standing, as this Court explained in the first appeal, rests on three allegations: (1) its communications traverse every international internet backbone link connecting the United States with the rest of the world; (2) the government allegedly conducts Upstream surveillance on at least one such link; and (3) wherever Upstream surveillance occurs, the government allegedly must copy *everything* (including any Wikimedia communications) because of what plaintiff describes as "the technical rules of how the [i]nternet works" 857 F.3d at 210-11.

1. Plaintiff says its communications transit every cross-border cable connecting the U.S. to other countries.

On remand, to support the first element of that theory, plaintiff introduced an opinion from Scott Bradner, an expert on internet communications, stating that, due to the number and geographic distribution of Wikimedia's internet communications,

Wikimedia's communications traverse "every circuit carrying public [i]nternet traffic on every international cable connecting the U.S. to other countries." JA 1043.

Importantly, Bradner does not make the broader claim that Wikimedia's communications traverse every internet circuit in the United States, or even every U.S. circuit that may carry communications ultimately destined to go abroad (or come from there)—*i.e.*, every U.S. circuit *carrying* international communications. Instead, Bradner states only that Wikimedia's communications are carried on every one of a very specific and relatively small set of circuits carrying public internet traffic on the cross-border (and mostly transoceanic) fiber optic cables connecting the domestic internet backbone to the rest of the world. *See* JA 992-94 (maps). Bradner's opinion thus tracks the complaint, in which plaintiff alleged its communications are carried on every one of a "relatively small number of international chokepoints." JA 57.

While not conceding the matter, for purposes of summary judgment the government did not dispute Bradner's statement that Wikimedia's communications would transit over "every circuit carrying public [i]nternet traffic on every international cable connecting the U.S. to other countries." JA 1043.

2. Plaintiff has no evidence that the government conducts surveillance on at least one such location.

Plaintiff failed to introduce evidence that Upstream surveillance occurs on at least one "circuit carrying public [i]nternet traffic on every international cable connecting the U.S. to other countries." JA 1043.

The district court correctly noted that none of the evidence that plaintiff put forward supported that conclusion. JA 4093-94. Plaintiff pointed to a declassified FISC opinion from 2011, which states that, according to a still-classified and privileged government filing, "NSA will acquire a wholly domestic 'about' communication"—that is, a communication *about* a targeted selector, rather than a communication *to* or *from* the selector—"if the transaction containing the communication is routed through an international [i]nternet link being monitored by NSA." JA 2676. That statement does not support plaintiff's theory. On its own terms, it says only that some "about" communications would be acquired *if* NSA were monitoring what the opinion referred to as an "international [i]nternet link." That conditional statement is not evidence of the existence of the conduct described after the word "if."[3] Consistent with the state-secrets privilege, an NSA deposition witness repeatedly refused to state whether NSA monitors "international [i]nternet links" or did so in 2011. JA 466-75.

Moreover, as the district court correctly concluded, plaintiff failed to identify evidence that the phrase "international [i]nternet link," as used in the FISC opinion, referred to the same thing that plaintiff says in the first element of its theory would carry Wikimedia communications: the relatively small set of circuits carrying public internet traffic on the chokepoint cables connecting the United States to the rest of

[3] Moreover, as the court noted, 'about' collection ended in 2017, so "at least the conclusion of this conditional statement is no longer accurate today." JA 4094 n.38.

the word. When plaintiff asked the NSA witness what the FISC opinion meant by "international [i]nternet link," the witness testified that the "NSA has an understanding of this term that," unlike other terms used in the industry, "is specific to how Judge Bates described it" in the FISC opinion, and that that specific understanding is a state secret. JA 447; *see* JA 226.

The district court thus correctly concluded that the NSA witness's testimony did not support the second element of plaintiff's theory because it "cannot be known without violation of the state secrets privilege" whether the phrase "international [i]nternet link" as used in the 2011 FISC opinion refers to the same thing at issue in the first element of plaintiff's theory. JA 4093-94. (Plaintiff's opening brief does not mention the district court's ruling on this point, much less argue that the court erred or explain how, Br. 25-27, and plaintiff has thus forfeited any opportunity to do so, *Grayson O Co. v. Agadir Int'l LLC*, 856 F.3d 307, 316 (4th Cir. 2017).)

There is thus no evidence in the record that a reasonable jury could use to conclude that the government conducts Upstream surveillance on at least one circuit on a cross-border cable connecting the U.S. with other countries. The PCLOB report, which plaintiff references (Br. 26-27 & n.7), only discusses in general terms how Upstream surveillance acquires communications that are transiting through "circuits that are used to facilitate [i]nternet communications." JA 2475-76. The PCLOB report does not say that Upstream surveillance takes place with regard to

circuits *on cables connecting the U.S. with other countries*. Nor does it matter that, in plaintiff's and Bradner's view, it would "make sense" for the government to conduct surveillance on such international cables. JA 1003; Br. 26-27. The point of summary judgment is to test whether plaintiff has *evidence* that a reasonable fact-finder could rely on to find for plaintiff. It does not. An "allegation about what the NSA 'must' be doing" based on NSA's asserted incentives "lacks sufficient factual support to get 'across the line from conceivable to plausible.'" 857 F.3d at 214.

The district court nonetheless concluded, *sua sponte*, that a portion of Director Coats' public declaration invoking the state-secrets privilege supported the second element of plaintiff's theory. JA 4094. Plaintiff did not make that argument and does not support it on appeal. Br. 26. And for good reason, because the district court was mistaken. The Coats declaration reiterates what the government has already said: "NSA is monitoring at least one circuit carrying international [i]nternet communications." JA 186. That should be no surprise, as the point of Section 702 surveillance is to collect the communications of certain targeted non-U.S. persons located *abroad*. Crucially, Director Coats' statement that the government conducts Upstream surveillance on at least one circuit *carrying* international internet communications says nothing about whether the government conducts such surveillance at the so-called "chokepoints" that plaintiff says its communications traverse—the small number of cross-border (and mostly transoceanic) fiber optic

cables connecting the domestic internet backbone to the rest of the world—rather than any other location on the internet backbone.

Indeed, as the district court recognized, relying on the same Coats declaration, the location(s) at which Upstream surveillance occurs is a state secret. JA 712. That is why, as the court held, the NSA witness properly refused to testify regarding whether NSA conducts Upstream surveillance on "international [i]nternet links," and why the NSA witness properly refused to testify regarding the meaning of that phrase in the 2011 FISC opinion. Here, however, the court overlooked the distinction between any circuit anywhere on the U.S. internet backbone *carrying* international internet communications—that is, any domestic U.S. internet circuit carrying a packet of information ultimately destined to go abroad (or that came from abroad)—and the relatively few international chokepoints at which the U.S. internet backbone is connected by cross-border cables with the rest of the world, which are the only locations that, according to Bradner, all carry plaintiff's communications.[4]

[4] Plaintiff contends that the PCLOB report, which mentions "circuits" when describing Upstream, means to say the government monitors multiple "circuits." Br. 26-27. That discussion is irrelevant and incorrect. Plaintiff has no evidence that its communications traverse every internet "circuit," or that its communications traverse whatever circuit(s) it thinks the PCLOB was referring to. In any event, the report, by omitting clunky parentheses around the "s," does not thereby say that the government monitors more than one circuit. JA 4093; *cf.* 1 U.S.C. § 1 ("[W]ords importing the plural include the singular."). The location(s) of Upstream surveillance is a state secret, JA 712, and one that the PCLOB did not blithely disclose.

3. Wherever Upstream surveillance occurs, plaintiff has no evidence that such surveillance involves copying plaintiff's communications.

In any event, the district court correctly held that plaintiff failed to introduce evidence supporting the third element of its theory of standing. Plaintiff's complaint contended that, at any location where Upstream surveillance occurs, "the government must" as "a technical matter" be "copying and reviewing all the international text-based communications that travel across a given link." JA 57. That contention rested on an assertion about "the technical rules of how the [i]nternet works." 857 F.3d at 210. But, on remand, plaintiff was unable to support that allegation with any evidence, and plaintiff has now abandoned that allegation entirely.

In moving for summary judgment, the government introduced declarations by Dr. Henning Schulzrinne, an expert in internet technology. JA 719. Schulzrinne explained that there are "a number of technically feasible, readily implemented ways" to conduct Upstream surveillance "that would not involve NSA interaction with Wikimedia's online communications." JA 724. Some hypothetical means of conducting internet surveillance would, as plaintiff says, involve taking everything off of a monitored circuit by making an "identical copy of the communications stream," with the stream sent "elsewhere for processing to identify communications of interest," such as by scanning for targeted selectors. JA 743.

But this "copy-all-then-scan" approach is not the *only* means of conducting internet surveillance. Schulzrinne describes a "filter-then-copy-and-scan" approach,

JA 3414, that would use the routers already in place on the internet backbone to "selectively copy[] only those communications that are deemed more likely to include communications of interest." JA 744. Routers read the "headers" of packets of information flowing over the internet to determine what action to take with those packets (such as deciding where to send them to get them closer to their destination). JA 748. For internal business purposes, internet service providers also use routers to create a copy of certain communications. JA 746. The decision of what communications to selectively copy are based on whether the information in the "header" of a particular packet—such as source or destination IP addresses, or "port" or "protocol" numbers specifying what kind of communication is in the body of the packet—matches the criteria in an "access control list" on the router. JA 745-47. Using a "whitelisting" technique, only those packets with header information matching specified criteria are copied. A "blacklisting" technique copies all packets transiting the router except those that match specified criteria. JA 747-48.

As Schulzrinne explains, these methods could be used not only to copy certain packets for service providers' internal business use, but also to selectively copy packets of interest for a surveilling entity. By using this method to filter internet communications before selectively copying and scanning, the "NSA could conduct Upstream surveillance without intercepting, copying, reviewing, or otherwise interacting with communications of Wikimedia." JA 742. (Indeed, that would be true "regardless of where on the [i]nternet, or at how many locations, the NSA conducts

Upstream collection." *Id.*) The NSA could whitelist or blacklist around communications to or from Wikimedia's IP addresses, or it could blacklist the types of communications that Wikimedia alleges it engages in (such as communications using certain protocols). JA 3412; JA 753-59.

This is not, as plaintiff says, some kind of dubious "Wikimedia-avoidance theory." Br. 36. As the district court explained, the key point is that, "as a technical matter," NSA *could* blacklist or whitelist around "certain high-frequency, low-interest IP addresses" or other types of communications specified by information in a packet header "to minimize the collection of communications of little interest to the NSA," and "Wikimedia's IP addresses" or other header information encompassing Wikimedia's communications *could* be of low interest "to the NSA." JA 4100; *see* JA 3426. Thus, to implement this method, NSA would need to determine, based on packet headers, what packets are of particular interest for scanning for targeted selectors. Filtering out the communications involving high-volume, low-interest websites could "reduce (potentially by as much as 90 percent or more) the technological, logistical, and financial burdens of processing large volumes of unwanted web traffic." JA 4036.

Plaintiff concedes that filtering first is "technologically possible." JA 4100; *see* JA 928, 1019, 1022, 1029, 1038, 1053. As a result of that concession, as the district court correctly held, JA 4091, 4095-96, there is no triable issue of fact regarding the third element of the theory that plaintiff pled and litigated in this Court in the first

appeal: the allegation that, as a "technical matter" the government must be copying and reviewing "all" communications that travel across a monitored circuit, JA 57, because of "the technical rules of how the [i]nternet works," 857 F.3d at 210. That allegation is false, and plaintiff has rightly abandoned it.

Instead, plaintiff now modifies the third prong of its theory and speculates that (a) the government would choose to copy everything rather than filtering first, and (b), even if the government were filtering first, the government would not choose filtering criteria that exclude Wikimedia's communications. But, as the district court correctly held, plaintiff has no admissible evidence supporting either assertion, which rest on speculation about NSA's priorities, capabilities, and mission requirements.

a. Plaintiff has no evidence NSA has chosen to copy everything rather than filter first.

i. Plaintiff chiefly points to a sentence from a declassified FISC opinion from 2011 (the same one discussed above), which characterizes a still-classified government filing as saying that the government "will acquire a wholly domestic 'about' communication if the transaction containing the communication is routed through" a part of the internet backbone hypothetically monitored by NSA. JA 2676. Bradner and Schulzrinne both agree that, as a technological matter, NSA would, indeed, acquire at least some such communications if it were using a filter-then-copy-and-scan approach. JA 3893, 3918; JA 4024. There is thus no inconsistency between the statement in the FISC opinion and a filter-then-copy-and-scan approach.

Bradner says the two are inconsistent because filtering first would result in NSA missing *some* of the wholly domestic "about" communications at issue, "which would not be consistent with the FISC statement that *all* 'about' communications '*will*' be acquired." JA 3894 (first emphasis added). That erroneous conclusion is not rooted in any technological expertise or factual basis, Fed. R. Evid. 702, but rather a misreading of the FISC opinion. The FISC opinion doesn't say that "all" such communications will be acquired; it says that "a" such communication will be acquired. JA 2676. And "will" should not be read to convert "a" into "all." The FISC did not make the statement at issue while characterizing the scope or completeness of such acquisitions, but rather while concluding that the *existence* of such acquisitions was not the result of a malfunction. JA 4025. And the FISC opinion elsewhere describes the same phenomenon by saying NSA "*may* acquire" such communications. JA 2666 n.34 (emphasis added).[5]

ii. Plaintiff also points to what it calls "a set of technical and practical necessities" that, in its view, counsel in favor of NSA adopting a copy-all-then-scan

[5] It is not true, as plaintiff insists, that this other passage refers to a "slightly different phenomenon." Br. 29 n.8. Both passages discuss the technical reasons why wholly domestic communications may be acquired. It does not matter that one passage says the government "will acquire a wholly domestic 'about' communication," while the other says the government "may acquire wholly domestic communications" (omitting "about"). JA 2666 n.34, 2676. There is no reason to think the FISC meant to say that the acquisition of "wholly domestic communications" in general (including "about" communications) was only a possibility, but the collection of wholly domestic "about" communications was a certainty. JA 4026 n.1.

approach. Br. 29. But the only "necessity" discussed in the opening brief is the mistaken assertion that there must be many thousands of Upstream surveillance targets, some of whom plaintiff says "move around," and that it is therefore "impossible for the NSA to know in advance which packets belong to its targets and which do not," for filtering purposes. Br. 30. Plaintiff's mistaken assertion rests on speculation about the number, nature, and behavior of Upstream surveillance targets and NSA's surveillance capabilities and priorities—all of which are classified state secrets about which plaintiff and Bradner have no knowledge or expertise.

As Schulzrinne explains, and as Bradner does not dispute, it is technologically feasible for NSA to acquire information about the IP addresses its targets use to communicate using Upstream, and programs other than Upstream, in order to determine what IP addresses to whitelist for Upstream collection. JA 4031. Plaintiff's assertion that there are too many Upstream targets for such a system to be practical rests on bare speculation about how many Upstream targets there are. And Bradner gives "no factual, technical basis for concluding that the number of the NSA's Upstream targets"—whatever that number may be—"would make whitelisting unworkable." JA 4032. Only NSA knows the number of Upstream targets, or the extent to which the IP addresses its targets use to communicate might change due to alleged geographic mobility. In any event, even if some targets move around, and even if there are many targets, there is no technological impediment to using whitelists

to conduct Upstream surveillance, as it is undisputed that NSA could use automated methods and publicly available information to learn about and whitelist all IP addresses associated with a given e-mail address, or that NSA could whitelist blocks of IP addresses associated with specific geographic areas. JA 4033.

iii. Plaintiff also asserts that copying everything would be more "comprehensive" than filtering first, and plaintiff believes (without evidence) that NSA therefore would choose to copy everything. Br. 30-31. The sole basis for plaintiff's claim that NSA values comprehensiveness, seemingly over all other possible considerations, is a single sentence repeated twice in the PCLOB report characterizing Upstream surveillance in general terms. There, the PCLOB says that so-called "about" collection is "largely an inevitable byproduct of the government's efforts to comprehensively acquire communications that are sent to or from its targets." JA 2449, 2562.

"Comprehensive" need not mean "exhaustive." And even if PCLOB's word choice supported an inference that NSA had a general aspiration to acquire literally *all* communications involving its targets, it does not support a conclusion that such a desire would override all other considerations. As Schulzrinne explains, and as Bradner does not dispute, there are "technical, logistical, and financial hurdles," "resource constraints," and "trade-offs" with other "competing mission priorities" that would "stand in the way" of collecting literally all communications involving targets. JA 3437. The relevant question, for NSA, is at what point the costs

"outweigh the marginal benefit of potentially discovering still further communications of its targets in some as-yet unexplored stream." *Id.* The answer to that question depends on what weight NSA assigns to various considerations, something outside Bradner's knowledge and field of expertise. JA 4029.

Plaintiff cannot invoke an inchoate goal of "comprehensiveness," assume without evidence that NSA values that goal above all else, and thereby convince a reasonable fact-finder that the government is copying everything rather than filtering first. Indeed, this Court already held as much in the first appeal in this case. There, the Court explained that "in the Dragnet allegation, Plaintiffs seek to use the theory governing [i]nternet 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." 857 F.3d at 214. The Court should apply the same reasoning here. *See Obama v. Klayman*, 800 F.3d 559, 567 (D.C. Cir. 2015) (Williams, J., concurring) (though NSA's collection was allegedly "comprehensive," "there are various competing interests that may constrain" the government's implementation); *id.* at 569-70 (Sentelle, J., agreeing with Judge Williams).

iv. Finally, the grab-bag of remaining items that plaintiff mentions are consistent with NSA using either proposed method of Upstream surveillance, and are thus not evidence that the government is copying everything. PCLOB may say that digital technology allows NSA to "examine the contents of all transmissions passing

through collection devices," JA 2561, and a treatise (one never entered into evidence) may make the same statement about a "collection point." Br. 31-32. But those statements say nothing about whether the stream of communications going into such a collection device or point includes everything from a monitored internet circuit or only filtered communications. Similarly irrelevant is whatever method the United Kingdom allegedly uses to conduct surveillance, Br. 32, as that not only has no bearing on what NSA does, but, in any event, public descriptions of U.K. surveillance are consistent with either copying everything or filtering first. JA 3434-35, 4043-44. And it is irrelevant that the government may copy whole communication streams entering federal government computer networks to detect unauthorized intrusions (a system called EINSTEIN 2.0), JA 3161, because underlying differences in the purposes and size of EINSTEIN 2.0 and Upstream mean that the methods used to implement the one do not provide insight into implementation of the other. JA 3435-36. Indeed, Bradner does not rely on EINSTEIN 2.0 to conclude that Upstream likely involves copying everything. JA 3934-35.

b. Plaintiff has no evidence regarding what criteria NSA would use to filter (if it does filter).

Plaintiff also fails to identify evidence that, if communications are first filtered for those likely to be of intelligence value, Wikimedia's communications would be among those NSA copies and scans. That failure is unsurprising, because the relevant information about NSA's priorities and intelligence interests is a state secret.

i. Plaintiff speculates that, even if the government blacklists some IP addresses, it would not blacklist Wikimedia's and lose access to any communications between Wikimedia and NSA targets. Br. 35-36. But plaintiff has no knowledge about, and certainly no evidence regarding, the reading habits of NSA's targets or the value NSA would place on knowing which Wikipedia articles any targets might read.[6] Plaintiff's brief also cites, without elaboration (Br. 36), a portion of Bradner's declarations in which he identified a small number of hypothetical scenarios in which some Wikimedia communications might be collected even if the government blacklisted Wikimedia's IP addresses. JA 1057. But, as the district court correctly held, plaintiff presented no evidence about the existence of those scenarios, much less any evidence that communications in those scenarios would be so numerous as to cross all international internet links. JA 4103-04 & n.55; *see also* JA 3439-44, 4044-46. Plaintiff's brief does not mention those conclusions, or argue they were erroneous.

Plaintiff also speculates that the government would not whitelist a set of IP addresses while excluding all others, contending that NSA would not want to create possible "blind spots." Br. 35. But only NSA knows whether surveillance conducted on a circumscribed set of communications would fulfill operational criteria, and what kinds of gaps NSA would deem significant.

[6] Plaintiff asserts that blacklisting Wikimedia's IP addresses, alone, would not "measurabl[y]" reduce the load on NSA systems. Br. 36; JA 3912-13. But Schulzrinne explains, and Bradner does not dispute, that blacklisting a broader set of high-volume, low-value sites would significantly reduce the load. JA 4035-36.

Plaintiff further asserts, with no explanation in its brief, that whitelisting IP addresses is "contradicted by the NSA's 'about' collection." Br. 35. Related to the "will acquire" discussion above, but this time focusing on NSA's alleged goal of comprehensiveness rather than the word "will," Bradner says that a whitelisting method would result in the collection of *some* "about" communications, but would not *comprehensively* collect "about" communications. JA 3918. But Bradner doesn't know whether Upstream is meant to comprehensively acquire "about" communications. Notably, the PCLOB report describes "about" communications as a "byproduct" of looking for to/from communications. JA 2449; *see* JA 4038-39.

ii. Plaintiff similarly speculates that the government would not want to blacklist certain *types* of communications, like those using protocols used to display most websites (HTTP or HTTPS). But plaintiff has no evidence about what types of communications NSA finds of particular intelligence interest.

Plaintiff argues (Br. 35) that the government has disclosed in a FISC filing that Upstream collects some "web activity," JA 2920, which, Bradner says, includes HTTP and HTTPS communications, JA 1034-35. Plaintiff asserts that the government could thus not be blacklisting HTTP and HTTPS communications. But Schulzrinne explains that the government could *generally* blacklist HTTP and HTTPS while still whitelisting packets to or from the IP addresses of certain websites, thus capturing *some* HTTP and HTTPS communications (and thus, on Bradner's view, some "web activity") without capturing Wikimedia's communications. JA 3425. Bradner does

not dispute that technological possibility. JA 3928. And neither he nor plaintiff can do anything other than speculate as to whether the government uses such a method.

Plaintiff similarly asserts (Br. 35) that blacklisting packets with encrypted contents would be inconsistent with FISC-approved minimization procedures that allow NSA to retain encrypted communications obtained under Section 702. JA 3204. But the government has acknowledged *two* types of Section 702 surveillance. Plaintiff identifies no evidence NSA collects encrypted communications through Upstream.

c. The district court correctly applied the summary-judgment standard.

Plaintiff argues that the court required plaintiff to "show that the NSA must be surveilling its communications as a technological necessity." Br. 37. Not true. The court correctly noted that "technological necessity" was plaintiff's own longstanding theory, but that plaintiff had since acknowledged there are at least *two* technologically feasible means of implementing Upstream. JA 4079, 4084, 4100. The court then evaluated plaintiff's fallback theory—that the government chose to use a method that would result in copying Wikimedia's communications—and correctly held that plaintiff identified no admissible evidence supporting that allegation. JA 4096-4105. That was the correct standard.

Plaintiff also contends that the court erred in failing to credit some of Bradner's opinions. Br. 38-40. The court credited opinions that were rooted in Bradner's expertise about internet communications. But, as the court correctly noted, some of

Bradner's opinions had no "foundation in technology" and instead rested on bare speculation "about the NSA's surveillance practices and priorities and the NSA's resources and capabilities." JA 4097. The latitude given to experts to offer opinions "is premised on an assumption that [an] expert's opinion will have a reliable basis in the knowledge and experience of [the expert's] discipline." *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 592 (1993). For that reason, a "reliable expert opinion must [not] be based … on belief or speculation." *Nease v. Ford Motor Co.*, 848 F.3d 219, 231 (4th Cir. 2017) (alterations in original). The court thus did not abuse its discretion in holding that Bradner's opinions resting on "speculative assumptions" about the NSA's "surveillance practices and priorities" and its "resources and capabilities" are inadmissible under Federal Rule of Evidence 702. JA 4097-98 & n.44.

Plaintiff faults the government for not introducing evidence regarding whether NSA actually filters plaintiff's communications. Br. 33. But plaintiff, not the government, bears the burden of introducing admissible evidence of standing. *Clapper*, 568 U.S. at 412 n.4. That Schulzrinne did not opine about which of multiple feasible options NSA would decide best fit its classified operational needs and resources only underscores why his declarations are admissible in their entirety, while Bradner's are not. And that plaintiff seeks to defeat summary judgment based on Bradner's speculation about NSA's priorities, while demanding the government introduce highly classified evidence, only underscores how further adjudication would threaten to disclose state secrets, as discussed below in Part III.

B. Plaintiff's Other Arguments About Standing Also Fail.

Having failed to identify evidence showing its communications are copied, plaintiff tries to lower the bar. It argues that it must show only a "substantial risk" of future harm plus costly actions taken to mitigate risk. Br. 22, 62, 65. But the Supreme Court rejected an "objectively reasonable likelihood" standard for cases challenging alleged surveillance in *Clapper*, 568 U.S. at 410. And plaintiff here does not even allege uncertain *future* events, *Beck v. McDonald*, 848 F.3d 262, 273-76 (4th Cir. 2017), but rather alleges actual copying from an ongoing program. In any event, "to the extent that the 'substantial risk' standard is relevant and is distinct from the 'clearly impending' requirement" regarding future harm, plaintiff "fall[s] short of even that standard, in light of the attenuated chain of inferences necessary to find harm here" on the thin summary-judgment record. *Clapper*, 568 U.S. at 414 n.5. The district court thus correctly held that plaintiff failed to satisfy both standards. JA 4088-89 n.30.

1. Plaintiff points to an alleged drop in readership of certain Wikipedia articles and to its own decision to pay money to encrypt its communications. Br. 63-64. Plaintiff contends that both alleged injuries were "driven by the revelations" about government surveillance in June 2013. Br. 64.

These alleged injuries rest on subjective and speculative fears of surveillance in general, not on any reaction to actual Upstream surveillance of Wikimedia (if any), and are therefore foreclosed as a matter of law by *Clapper*, 568 U.S. at 415-18 & n.7.

This Court held as much in the first appeal, when it affirmed dismissal of all plaintiffs' claims (including Wikimedia's) predicated on the "dragnet" theory. "[I]t follows" from plaintiffs' inability to "show that the NSA is intercepting their communications," this Court explained, that plaintiffs also lacked standing to challenge surveillance under alternative theories of injury 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." 857 F.3d at 216 (second alteration in original). Plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based" on "fears of hypothetical future harm." *Id.* The district court correctly applied the same reasoning here, after concluding that Wikimedia had failed to substantiate its allegation that its communications were subject to surveillance. JA 4114-17.

2. Finally, plaintiff urges this Court to decide that, "[i]f Wikimedia has standing, it also has third-party standing to assert the rights" of others. Br. 66. That argument fails because Wikimedia lacks standing. Moreover, Wikimedia has not shown that any particular third party's communications are subject to surveillance, and plaintiff cannot assert the supposed rights of people who are not themselves "among the injured." *Lujan*, 504 U.S. at 563. In any event, as the district court correctly held, the relationship between Wikimedia and those who visit and contribute to its websites is not the kind of "protected, close relationship[]" to which third-party standing might apply, such as certain doctor-patient relationships. JA 4117 & n.65; *Singleton v. Wulff*, 428 U.S. 106, 113-14 (1976). For those who visit or contribute to

particular webpages with content that raises privacy concerns, putative plaintiffs need not disclose the content of those sensitive communications to bring their own suits, but rather only the simple facts that they are internet users who visit Wikimedia websites in general. JA 4118 & n.67.

III. The District Court Correctly Held that Dismissal Was Also Required to Protect State Secrets.

A. Dismissal is independently required to protect state secrets where, as here, "the circumstances make clear that privileged information will be so central to the litigation that any attempt to proceed will threaten that information's disclosure." *El-Masri*, 479 F.3d at 308. This Court has identified three "examples" of when dismissal is required, such as when a plaintiff cannot "prove the prima facie elements" of a claim "without privileged evidence," when a defendant cannot "properly defend [itself] without using privileged evidence," and when "further litigation would present an unjustifiable risk of disclosure." *Abilt*, 848 F.3d at 313-14.

The district court correctly held that dismissal is required here because "the operational details of the Upstream collection process and whether any of Wikimedia's international [i]nternet communications have been copied" is "central to the litigation of Wikimedia's standing." JA 4111. The government could not "properly defend" itself without using privileged information, as "virtually any conceivable response to [Wikimedia's] allegations" regarding standing "would disclose privileged information" about Upstream. JA 4110.

The court noted (JA 4110-11) that "the whole object of" further adjudication would be "to establish a fact that is a state secret," *Sterling*, 416 F.3d at 348—namely, how NSA conducts Upstream surveillance and whether it copies Wikimedia's communications. As the discussion in Part II.A shows, any trial here would require litigation of, at the very least, (i) whether NSA conducts Upstream surveillance at one or more international internet links, and (ii) whether NSA uses a "copy-all-then-scan" approach or whether it filters first (and, if so, what criteria it uses). "[S]uch information forms the very basis of the factual disputes in this case." *Id.* at 346. "Due to the nature of the question presented in this action and the proof required by the parties to establish or refute the claim, the very subject of this litigation is itself a state secret." *Fitzgerald*, 776 F.2d at 1243.

If a trial were held, the government would have two options: either (1) present highly classified evidence about the subjects, methods, location(s), scope, and capabilities of Upstream surveillance in order to rebut plaintiff's claims, if they are in error, or (2) remain silent in the face of plaintiff's claims, whether true or not, to avoid more harmful disclosures, thereby either disclosing by implication the classified facts the privilege is supposed to protect (if plaintiff's allegations are correct), or allowing the Court to proceed in error (if they are not). The state-secrets doctrine solves that dilemma. "[D]ismissal follows inevitably when," as here, "the sum and substance of the case involves state secrets." *Sterling*, 416 F.3d at 347. The district court thus

correctly held that dismissal was necessary to protect state secrets. *See Halkin*, 598 F.2d at 9 (claims of unlawful NSA surveillance dismissed to protect state secrets).

B. 1. Plaintiff maintains that state secrets are not "central" to this case because, plaintiff asserts, it needs to prove only a "*substantial risk*" of copying. Br. 62. As explained above in Part II.B, the "substantial risk" standard is inapplicable here. Even if it were the correct standard, privileged information would still inevitably be at issue (and at risk of disclosure) in litigating standing. NSA's actual (and privileged) surveillance methods are just as relevant to whether there is a "substantial risk" of copying as to whether such copying actually occurs.

2. Plaintiff contends that the district court erred in dismissing the case without first reviewing state-secrets *in camera* to determine "the validity" and "existence" of what plaintiff calls the government's "*hypothetical* defense"—that is, to determine whether, in fact, the government uses a filter-then-copy-and-scan technique that avoids Wikimedia's communications. Br. 59-61.

That suggestion is foreclosed by binding precedent. In *El-Masri*, this Court outlined "possible defenses" the government might offer, including factual attacks on plaintiff's allegations, and ordered dismissal because each defense would expose state secrets. 479 F.3d at 310. In so holding, the Court made clear that it did "not, of course, mean to suggest that any of these *hypothetical* defenses represents *the true state of affairs* in this matter, but they illustrate that virtually any conceivable response … would disclose privileged information." *Id.* (emphases added).

Plaintiff's suggestion is also contrary to core state-secrets principles. Privileged evidence is "remove[d] … from the proceedings entirely." *El-Masri*, 479 F.3d at 306. A "court should not jeopardize the security which the privilege is meant to protect by insisting upon an examination of the evidence, even by the judge alone, in chambers." *Id.* at 311. Plaintiff's approach would expose state secrets, as the publicly announced result of the *in camera* review (dismissing the case, or not) would reveal how Upstream is implemented and whose communications are or are not copied. The district court thus correctly held that dismissal was required to protect state secrets.

CONCLUSION

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

Respectfully submitted,

ETHAN P. DAVIS
Acting Assistant Attorney General

H. THOMAS BYRON III
s/ Joseph F. Busa
JOSEPH F. BUSA
Attorneys, Appellate Staff
Civil Division, Room 7537
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530
(202) 305-1754
Joseph.F.Busa@usdoj.gov

August 2020

CERTIFICATE OF COMPLIANCE

This brief complies with the word limit prescribed by Order of this Court on July 20, 2020 because it contains 14,999 words. This brief also complies with the typeface and type-style requirements of Federal Rule of Appellate Procedure 32(a)(5)-(6) because it was prepared using Microsoft Word 2016 in Garamond 14-point font, a proportionally spaced typeface.

s/ Joseph F. Busa
Joseph F. Busa
Counsel for Defendants-Appellees

CERTIFICATE OF SERVICE

I hereby certify that on August 7, 2020, I electronically filed the foregoing brief with the Clerk of the Court for the United States Court of Appeals for the Fourth Circuit by using the appellate CM/ECF system. Participants in the case are registered CM/ECF users, and service will be accomplished by the appellate CM/ECF system.

s/ Joseph F. Busa
Joseph F. Busa
Counsel for Defendants-Appellees

ADDENDUM

TABLE OF CONTENTS

Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 *et seq.*

§ 1801. Definitions

. . .

(k) "Aggrieved person" means a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.

. . .

§ 1806. Use of information

. . .

(c) Notification by United States. Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

. . .

(e) Motion to suppress. Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that—

(1) the information was unlawfully acquired; or

(2) the surveillance was not made in conformity with an order of authorization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(f) In camera and ex parte review by district court. Whenever a court or other authority is notified pursuant to subsection (c) or (d), or whenever a motion is made pursuant to subsection (e), or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

(g) Suppression of evidence; denial of motion. If the United States district court pursuant to subsection (f) determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(h) Finality of orders. Orders granting motions or requests under subsection (g), decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

. . .

§ 1881a. Procedures for targeting certain persons outside the United States other than United States persons ["Section 702"]

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

(b) Limitations. An acquisition authorized under subsection (a)—

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

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

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

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

(5) may not intentionally acquire communications that contain a reference to, but are not to or from, a target of an acquisition authorized under subsection (a), except as provided under section 103(b) of the FISA Amendments Reauthorization Act of 2017; and

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

. . .

(d) Targeting procedures.

(1) Requirement to adopt. The Attorney General, in consultation with the Director of National Intelligence, shall adopt targeting procedures that are reasonably designed to—

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

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

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

(e) Minimization procedures.

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

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

. . .

. . .

(g) Guidelines for compliance with limitations.

(1) Requirement to adopt. The Attorney General, in consultation with the Director of National Intelligence, shall adopt guidelines to ensure—

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

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

(2) Submission of guidelines. The Attorney General shall provide the guidelines adopted in accordance with paragraph (1) to—

(A) the congressional intelligence committees;

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

(C) the Foreign Intelligence Surveillance Court.

(h) Certification.

(1) In general

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

. . .

(2) Requirements. A certification made under this subsection shall—

(A) attest that—

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

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

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

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

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

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

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

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

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

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

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

. . .

. .

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

(i) Directives and judicial review of directives.

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

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

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

. . .

(4) Challenging of directives

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

. . .

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

. . .

(5) Enforcement of directives

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

. . .

(6) Appeal

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

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

(j) Judicial review of certifications and procedures.

(1) In general

(A) Review by the Foreign Intelligence Surveillance Court. The Foreign Intelligence Surveillance Court shall have jurisdiction to review a certification submitted in accordance with subsection (g) and the targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1), and amendments to such certification or such procedures.

. . .

(2) Review. The Court shall review the following:

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

(B) Targeting procedures. The targeting procedures adopted in accordance with subsection (d) to assess whether the procedures are reasonably designed to—

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

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

(C) Minimization procedures. The minimization procedures adopted in accordance with subsection (e) to assess whether such procedures meet the

definition of minimization procedures under section 1801(h) of this title or section 1821(4) of this title, as appropriate.

. . .

. . .

(4) Appeal

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

. . .

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

. . .

. . .