No. 22-190

In the Supreme Court of the United States

WIKIMEDIA FOUNDATION, PETITIONER

v.

NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE, ET AL.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

BRIEF FOR THE RESPONDENTS IN OPPOSITION

ELIZABETH B. PRELOGAR
Solicitor General
Counsel of Record
BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General
SHARON SWINGLE
JOSEPH F. BUSA
Attorneys

Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217

QUESTIONS PRESENTED

1. Whether a court may dismiss an action without prejudice under the state-secrets doctrine, where the parties could not fairly litigate matters on which the plaintiff has the burden of proof and any judicial resolution of those matters would jeopardize state secrets, the disclosure of which reasonably could be expected to cause significant harm to the national security.

2. Whether a court, in order to dismiss a case on state-secrets grounds, must first conduct an *in camera* and *ex parte* adjudication using evidence protected by the state-secrets privilege and determine based on that evidence that the party seeking dismissal presents a defense on which it would prevail if the litigation were to proceed.

ADDITIONAL RELATED PROCEEDING

United States Court of Appeals (4th Cir.):

Wikimedia Found. v. *National Sec. Agency/Central Sec. Serv.*, No. 15-2560 (May 23, 2017)

TABLE OF CONTENTS

Page

Opinions below 1
Jurisdiction 1
Statement 1
Argument 13
Conclusion 31

TABLE OF AUTHORITIES

Cases:

Armour & Co. v. *Wantock*, 323 U.S. 126 (1944) 21
Bareford v. *General Dynamics Corp.*, 973 F.2d 1138 (5th Cir. 1992), cert. denied, 507 U.S. 1029 (1993) 30
Clapper v. *Amnesty Int'l USA*, 568 U.S. 398 (2013) 2, 29
Cohens v. *Virginia*, 19 U.S. (6 Wheat.) 264 (1821) 21
Department of the Navy v. *Egan*, 484 U.S. 518 (1988) 23
Emich Motors Corp. v. *General Motors Corp.*, 340 U.S. 558 (1951) 21
FBI v. *Fazaga*, 142 S. Ct. 1051 (2022) 10, 24, 28
Fitzgerald v. *Penthouse Int'l, Ltd.*, 776 F.2d 1236 (4th Cir. 1985) 30
General Dynamics Corp. v. *United States*, 563 U.S. 478 (2011) 24
Haig v. *Agee*, 453 U.S. 280 (1981) 23
Landgraf v. *USI Film Prods.*, 511 U.S. 244 (1994) 21
Lujan v. *Defenders of Wildlife*, 504 U.S. 555 (1992) 15
Martin v. *Mott*, 25 U.S. (12 Wheat.) 19 (1827) 22
McCardle, Ex parte, 74 U.S. (7 Wall.) 506 (1869) 16
Merck Sharp & Dohme Corp. v. *Albrecht*, 139 S. Ct. 1668 (2019) 21

Cases—Continued: Page

Mohamed v. *Jeppesen Dataplan, Inc.*, 614 F.3d 1070 (9th Cir. 2010), cert. denied, 563 U.S. 1002 (2011) ... 27, 30

Redacted, No. [Redacted], 2011 WL 10945618 (FISA Ct. Oct. 3, 2011) ... 11, 18-20

Reiter v. *Sonotone Corp.*, 442 U.S. 330 (1979) ... 21

Sealed Case, In re, 494 F.3d 139 (D.C. Cir. 2007) ... 27

Steel Co. v. *Citizens for a Better Env't*, 523 U.S. 83 (1998) ... 16

Tenet v. *Doe*, 544 U.S. 1 (2005) ... 16, 24-26

Totten v. *United States*, 92 U.S. 105 (1876) ... 22, 23, 25, 26, 28

United States v. *Burr*, 25 F. Cas. 30 (C.C.D. Va. 1807) ... 22

United States v. *Nixon*, 418 U.S. 683 (1974) ... 23

United States v. *Reynolds*, 345 U.S. 1 (1953) ... 7, 22, 23, 26, 28

United States v. *Zubaydah*, 142 S. Ct. 959 (2022) ... 30

Weinberger v. *Catholic Action of Haw./Peace Educ. Project*, 454 U.S. 139 (1981) ... 23-26, 28

Constitution, statutes, and rule:

U.S. Const.:

Art. III ... 5, 7-11, 14-16, 22, 27

Amend. IV ... 4

FISA Amendments Act of 2008, Pub. L. No. 110-261, sec. 101(a)(2), § 702, 122 Stat. 2438-2448 ... 2

FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, § 103(b), 132 Stat. 10-13 (50 U.S.C. 1881a note) ... 5

Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. 1801 *et seq.* ... 2

Statutes and rule—Continued: Page

50 U.S.C. 1801(e) 3
50 U.S.C. 1806(f) 6, 9, 10, 13
50 U.S.C. 1881a (§ 702) 2-5, 17, 18, 29
50 U.S.C. 1881a(a) 3
50 U.S.C. 1881a(b)(1) 3
50 U.S.C. 1881a(b)(2) 3
50 U.S.C. 1881a(b)(3) 3
50 U.S.C. 1881a(b)(5) 5
50 U.S.C. 1881a(b)(6) 3
50 U.S.C. 1881a(c)(1)(A) 3
50 U.S.C. 1881a(d)(1) 3
50 U.S.C. 1881a(h)(2)(A) 3
50 U.S.C. 1881a(i)(1)(A) 3
50 U.S.C. 1881a(i)(5)(A) 3
50 U.S.C. 1881a(j)(2) 3
50 U.S.C. 1881a(j)(3) 3
50 U.S.C. 1881a(m)(4) 5
National Environmental Policy Act of 1969, 42 U.S.C. 4321 *et seq.* 25
42 U.S.C. 4332(2)(C) 25
42 U.S.C. 2000ee(a) 2
Sup. Ct. R. 10(a) 16

Miscellaneous:

Press Release, NSA/Cent. Sec. Serv., *NSA Stops Certain Section 702 "Upstream" Activities* (Apr. 28, 2017), https://perma.cc/BD7N-XUSF 5

In the Supreme Court of the United States

No. 22-190

WIKIMEDIA FOUNDATION, PETITIONER

v.

NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE, ET AL.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

BRIEF FOR THE RESPONDENTS IN OPPOSITION

OPINIONS BELOW

The opinion of the court of appeals (Pet. App. 1a-72a) is reported at 14 F.4th 276. The opinions of the district court (Pet. App. 73a-142a, 145a-179a) are reported at 427 F. Supp. 3d 582 and 335 F. Supp. 3d 772.

JURISDICTION

The judgment of the court of appeals was entered on September 15, 2021. A petition for rehearing was denied on March 29, 2022 (Pet. App. 274a-275a). On June 6, 2022, the Chief Justice extended the time within which to file a petition for a writ of certiorari to and including August 26, 2022, and the petition was filed on that date. The jurisdiction of this Court is invoked under 28 U.S.C. 1254(1).

STATEMENT

1. a. In the wake of the 9/11 attacks, the United States undertook a series of actions to obtain foreign-

intelligence information to protect the Nation from further attacks. See C.A. App. 2455-2458. Among other things, the President authorized the National Security Agency (NSA) to "collect the contents of certain international communications" through electronic surveillance, an activity that was later referred to as the Terrorist Surveillance Program. *Id.* at 2455; see *Clapper* v. *Amnesty Int'l USA*, 568 U.S. 398, 403 (2013). Over time, that activity and its relevant legal authority evolved. C.A. App. 2455-2458; see *Clapper*, 568 U.S. at 403-404.

As relevant here, in 2008, Congress amended the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. 1801 *et seq.*, by adding Section 702, which is codified at 50 U.S.C. 1881a. See FISA Amendments Act of 2008, Pub. L. No. 110-261, sec. 101(a)(2), § 702, 122 Stat. 2438-2448. That provision—referred to here as Section 1881a—governs the ongoing foreign-intelligence activities developed after the Terrorist Surveillance Program. C.A. App. 2444-2445, 2458-2459. The Privacy and Civil Liberties Oversight Board (PCLOB)—an independent government agency, 42 U.S.C. 2000ee(a)—has reviewed the relevant activities authorized by Section 1881a and has determined that they collect information that is "valuable and effective in protecting the nation's security and producing useful foreign intelligence." C.A. App. 2441.

Section 1881a establishes procedures for authorizing certain types of surveillance targeting non-United States persons located outside the United States when the acquisition involves obtaining foreign-intelligence information from, or with the assistance of, an electronic communication service provider. See *Clapper*, 568 U.S. at 404-406, 422 (discussing Section 1881a). Section 1881a provides that, "upon the issuance of an order" by the Foreign Intelligence Surveillance Court (FISC), the Attorney Gen-

eral and Director of National Intelligence (DNI) may jointly authorize the "targeting of persons reasonably believed to be located outside the United States" for a period of up to one year to acquire "foreign intelligence information." 50 U.S.C. 1881a(a); see 50 U.S.C. 1801(e) (defining "[f]oreign intelligence information"). Section 1881a specifies that the authorized acquisition may not intentionally target any person known to be in the United States or any United States person reasonably believed to be outside the United States, 50 U.S.C. 1881a(b)(1) and (3), and may not target a person outside the United States "if the purpose * * * is to target a particular, known person reasonably believed to be in the United States," 50 U.S.C. 1881a(b)(2). The acquisition must be conducted in accordance with targeting procedures reasonably designed to ensure that it targets only "persons reasonably believed to be located outside the United States" and to prevent the intentional acquisition of "any communication as to which the sender and all intended recipients" are known to be located in the United States. 50 U.S.C. 1881a(c)(1)(A) and (d)(1). Section 1881a further requires that the acquisition be "conducted in a manner consistent with the [F]ourth [A]mendment." 50 U.S.C. 1881a(b)(6).

The Attorney General and the DNI must certify to the FISC that those and other requirements are satisfied, 50 U.S.C. 1881a(h)(2)(A), after which the FISC must review the certifications and associated procedures and enter an order approving them if the court determines that they satisfy all relevant requirements, 50 U.S.C. 1881a(j)(2) and (3). The Attorney General and DNI may then direct an electronic communication service provider to assist in the authorized acquisition. 50 U.S.C. 1881a(i)(1)(A) and (5)(A).

b. In 2015, petitioner, a nonprofit organization that operates the Wikipedia.org website, and other plaintiffs filed this action challenging the NSA's so-called "Upstream" internet surveillance activities authorized under Section 1881a. C.A. App. 36-95 (complaint). As relevant here, petitioner alleges that those activities have "intercept[ed], cop[ied], and review[ed]" petitioner's own internet communications while in "transit"; contends that Upstream surveillance under Section 1881a violates the Fourth Amendment; and seeks an injunction to prohibit "Upstream surveillance." *Id.* at 55, 93.

The PCLOB's public report (C.A. App. 2435-2630) explains that Upstream surveillance is labeled as such because it collects intelligence "in the flow of communications between communication service providers," which is "'upstream'" of the local service provider with which a targeted person interacts. *Id.* at 2474. To conduct Upstream surveillance, the government determines that a specific electronic communication "selector" (*e.g.*, an email address) is used by a non-United States person abroad who is targeted for foreign-intelligence surveillance, *id.* at 178 & n.2, 2460, 2471-2472, and transmits that selector "to a United States electronic communication service provider to acquire communications that are transiting through circuits that are used to facilitate [i]nternet communications," *id.* at 2475-2476; see *id.* at 2474. Such Upstream surveillance has been used to collect internet communications sent "to" or "from" a tasked selector. *Id.* at 2476. Upstream surveillance was also previously used to collect "so-called 'about' communications," *i.e.*, communications that were "about" a selector because each "contain[ed] the selector in the body

of the communication," *id.* at 2446, 2476, but that collection has been discontinued.[1]

The foregoing description of the "the Upstream collection process" is publicly available because the government "declassified" and disclosed certain limited information describing that intelligence activity "in general terms." C.A. App. 178; see *id.* at 183. More specific "operational details of Upstream collection," however, "remain highly classified." *Id.* at 178.

2. a. The district court initially dismissed petitioner's action at the pleading stage based on its determination that the complaint failed to establish any plaintiff's Article III standing to sue. Pet. App. 234a-271a. The court of appeals affirmed in part, vacated in part, and remanded, *id.* at 182a-233a, based on its view that petitioner's (but no other plaintiff's) pleading-stage allegations were sufficient, *id.* at 188a, 208a-215a.

b. In jurisdictional discovery on remand, petitioner sought evidence from the government—including "evidence concerning the scope and breadth of Upstream surveillance"—in connection with petitioner's standing theory. Pet. App. 154a. After the government objected to the discovery of several categories of information on

---

[1] In 2017, the NSA announced that it had discontinued Upstream "about" collection under Section 1881a. Press Release, NSA/Cent. Sec. Serv., *NSA Stops Certain Section 702 "Upstream" Activities* (Apr. 28, 2017), https://perma.cc/BD7N-XUSF. Congress later prohibited the intentional acquisition under Section 1881a of communications other than those "to or from" a surveillance target, unless the Attorney General and the DNI notify the congressional intelligence committees of their intent to implement "about" collection and comply with other statutory procedures. 50 U.S.C. 1881a(b)(5); FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, § 103(b), 132 Stat. 10-13 (50 U.S.C. 1881a note); cf. 50 U.S.C. 1881a(m)(4).

state-secrets grounds, *id.* at 154a-155a, the district court denied petitioner's motion to compel discovery. *Id.* at 145a-179a.

The district court first rejected petitioner's contention that procedures within a provision of FISA—50 U.S.C. 1806(f)—displace the state-secrets privilege. Pet. App. 156a-170a. The court determined that Section 1806(f)'s "procedures do not apply where, as here, [a litigant] has not yet established that it has been the subject of electronic surveillance." *Id.* at 157a, 170a; see also *id.* at 128a-132a (applying that determination at summary judgment).

The district court then determined that the government had properly asserted the state-secrets privilege and that the privilege foreclosed petitioner's requested discovery. Pet. App. 170a-179a. The court stated that it had conducted a "careful review" of the public, unclassified declaration of then-DNI Daniel R. Coats, who invoked the state-secrets privilege, and the classified declaration of NSA Deputy Director George C. Barnes, who provided additional classified details about the national-security harms of disclosure. *Id.* at 174a; see *id.* at 154a-155a. In his declaration (C.A. App. 171-189), the DNI stated that information about Upstream surveillance activities falling in seven general categories "is vital to the national security of the United States" and, if disclosed, "reasonably could be expected to cause serious damage, and in many cases exceptionally grave damage, to the national security." *Id.* at 174-175. The DNI explained that such disclosure could, *inter alia*, reveal to adversaries the extent of the government's ability to monitor their activities and compromise the NSA's vital ongoing intelligence-gathering activities. *Id.* at 184-185; see *id.* at 182-183.

The district court found that the government had properly invoked the state-secrets privilege and that "a reasonable danger" exists that disclosing the privileged information would expose "matters which, in the interest of national security, should not be divulged." Pet. App. 173a-174a (quoting *United States* v. *Reynolds*, 345 U.S. 1, 10 (1953)); see *id*. at 178a. The court found it "clear" that the seven categories of information identified by the DNI—including which "entities [are] subject to Upstream surveillance," the "operational details of the Upstream collection process," and the location or "locations" at which such collection is conducted—"fall[] squarely within the ambit of the state secrets privilege," given the "likel[ihood]" that their disclosure would cause national-security harm. *Id*. at 174a-175a.

c. The district court later granted the government summary judgment on two independent grounds, Pet. App. 73a-142a, and dismissed the case without prejudice, *id*. at 143a.

First, the district court determined that petitioner failed to proffer sufficient summary-judgment evidence regarding its Article III standing. Pet. App. 99a-120a, 137a-138a. The court stated that petitioner advanced a three-prong factual theory to attempt to show that the NSA conducts Upstream surveillance activity that "copie[s] and collect[s]" at least "some of [petitioner's] communications": Petitioner asserted that (i) petitioner's "communications almost certainly traverse every international Internet backbone link connecting the United States with the rest of the world"; (ii) "the NSA conducts Upstream surveillance at one or more points along the Internet backbone"; and (iii) "the NSA, for technical reasons, must be copying and reviewing all the text-based communications that travel across a given

Internet backbone link upon which it conducts Upstream surveillance." *Id.* at 100a-101a. The court determined that petitioner failed to establish a genuine issue of material fact on the third prong of that theory because "the summary judgment record" showed that "the NSA, in the course of Upstream surveillance, does not need to be copying any of [petitioner's] communications as a technological necessity." *Id.* at 101a; see *id.* at 106a-120a.

In analyzing the summary-judgment evidence, the district court discussed the "extensive" expert evidence in the case, Pet. App. 107a-119a; noted the "voluminous record" on unclassified matters relevant to Upstream surveillance, *id.* at 125a; and observed that in light of that evidence, petitioner's own expert acknowledged that it would be "technologically possible" for the NSA to conduct Upstream surveillance at "an international Internet circuit that transmits some of [petitioner's] communications" without "collect[ing] any of [petitioner's] communications," *id.* at 113a. The court emphasized that the so-called "practical grounds on which [petitioner's expert] reache[d] his conclusions" about the actual method of Upstream surveillance lacked "a non-speculative foundation in technology." *Id.* at 108a-109a. And the court ultimately concluded that petitioner could not establish its standing because "it is not true, as a technical necessity, that the NSA must be copying every text-based communication that traverses [an internet] circuit that the NSA monitors." *Id.* at 126a.

Second, the district court independently determined that, "[e]ven assuming *arguendo*" that petitioner proffered sufficient evidence to create a triable issue of fact for Article III standing, dismissal was warranted in light of the state-secrets doctrine. Pet. App. 120a-128a.

The court determined that petitioner's "standing cannot be fairly litigated any further without disclosure of [the] state secrets [that the doctrine] absolutely protect[s]." *Id.* at 120a. The court explained that even if petitioner had established "a *prima facie* case of its standing based solely on the public, unclassified record," the government could not fairly litigate that point "without using privileged evidence" and thus damaging the national security. *Id.* at 126a-127a. The court added that "if the issue of [petitioner's] standing were further adjudicated, 'the whole object of the adjudication . . . would be to establish * * * fact[s] that [are] state secret[s]' "—including "operational details of the Upstream collection process" and "the identity of parties whose communications" have been subject to surveillance—and that the state-secrets doctrine prohibits that result. *Id.* at 127a (citation and brackets omitted).

3. The court of appeals affirmed. Pet. App. 1a-72a. In separate opinions, two judges determined that the district court's summary judgment should be affirmed, but each based that conclusion on different grounds, neither of which speaks for a majority of the court. Judge Rushing, like the district court, concluded that petitioner failed to proffer sufficient evidence to establish Article III standing. *Id.* at 68a-72a. Judge Diaz, like the district court in its alternative ruling, concluded that the state-secrets doctrine required dismissal of petitioner's case. *Id.* at 52a-58a.

a. In Part II.B.2 of Judge Diaz's lead opinion (Pet. App. 1a-59a), a majority of the court of appeals agreed with the district court that Section 1806(f) did not displace the state-secrets privilege. *Id.* at 37a-52a (Part II.B.2); see *id.* at 68a (Rushing, J.) (agreeing with "Part II.B.2"). The majority explained that although this

Court had granted certiorari in *FBI* v. *Fazaga*, 142 S. Ct. 1051 (2022), to provide a "definitive answer" to the Section 1806(f) question, the majority had decided to resolve the issue itself before this Court rendered its decision in *Fazaga* in order to provide its analysis why Section 1806(f) does not displace the privilege in this case. Pet. App. 36a n.14. This Court later held in *Fazaga* that "[Section] 1806(f) does not displace the state secrets privilege." 142 S. Ct. at 1060.

Turning to the government's state-secrets-privilege assertion, Judge Diaz stated that petitioner did not "meaningfully dispute" that the government had properly asserted the "privilege for the seven categories of information" at issue; "agree[d] that 'there is a reasonable danger' to national security should these facts be disclosed"; and, for that reason, concluded that the government had properly invoked the privilege, which foreclosed petitioner's motion to "compel the government to produce" discovery. Pet. App. 53a-54a (citation omitted). Judge Rushing agreed that the privilege had been properly invoked, explaining that "[t]he Government's successful assertion of the state secrets privilege" to foreclose discovery "erected a significant hurdle for [petitioner's] effort to set forth specific facts" at summary judgment to establish Article III standing. *Id*. at 72a.

b. Judge Rushing then determined in her separate opinion (Pet. App. 68a-72a) that the district court had properly granted summary judgment to the government because petitioner had failed to carry its burden of proffering sufficient evidence of Article III standing. Like the district court, Judge Rushing concluded that petitioner had failed to proffer "technological facts, expert opinion, or other evidence" that might sufficiently support petitioner's factual theory that the NSA

conducts Upstream surveillance by "copying all traffic" —including at least some of petitioner's internet communications—that transit an international internet link that the NSA monitors. *Id.* at 69a.

Judge Rushing further observed that petitioner mistakenly sought to support its view of the facts with a passage in a declassified redacted 2011 FISC opinion that read: "Indeed, the government readily concedes that NSA will acquire a wholly domestic 'about' communication if the transaction containing the communication is routed through an international Internet link being monitored by NSA or is routed through a foreign server," *Redacted*, No. [Redacted], 2011 WL 10945618, at *15 (FISA Ct. Oct. 3, 2011). See Pet. App. 69a. Judge Rushing determined that the FISC's statement merely reflected that the "NSA was collecting communications containing tasked selectors * * * on the [international] circuits it monitored," and that "[n]othing in this statement or the [FISC's] surrounding analysis" supports the view that "NSA was collecting *all* such communications." *Id.* at 70a. Petitioner's contrary interpretation of the passage in the FISC's opinion, Judge Rushing explained, "fail[ed] to account for [the opinion's relevant] 'context'" and relied on an "unreasonable inference" from the statement. *Id.* at 69a (citation omitted).

A majority of the court of appeals disagreed with Judge Rushing on that point. In Part II.A.2 of Judge Diaz's lead opinion (Pet. App. 30a-35a), with which Judge Motz concurred (*id.* at 60a), the majority recognized that petitioner had "acknowledg[ed] that it's technically feasible to conduct Upstream surveillance without copying all communications on a monitored link" and, for that reason, petitioner no longer sought to establish Article III standing by showing that the NSA

copied and reviewed its communications as a matter of "technical necessity." *Id.* at 31a. The majority stated that petitioner instead sought to show that the NSA "by choice" is "copying all transactions on a monitored link," a factual assertion for which the majority found sufficient evidentiary support in the sentence in the FISC's opinion quoted above. *Ibid.* The majority concluded that there was a genuine issue of material fact on that issue because "reasonable inferences" could be drawn to interpret the relevant passage as reflecting that the "NSA [wa]s copying all transactions on a monitored link," *ibid.*, based on the majority's parsing of the 2011 FISC opinion's use of the "indefinite article, 'a,'" and the phrase "will acquire," *id.* at 32a-34a.

c. Judge Diaz, writing for himself, nevertheless concluded in Part II.B.3 of his opinion that the district court correctly granted summary judgment on the alternative ground that the state-secrets doctrine warranted dismissal of petitioner's case. Pet. App. 52a-58a (Part II.B.3).[2] Judge Diaz reasoned that where "any attempt to proceed [further in the litigation] will threaten disclosure of [state secrets], dismissal is the proper remedy." *Id.* at 54a (citation omitted). And in this case, he concluded, "state secrets are so central to the proceeding" that "further litigation would present an unjustifiable risk of disclosure." *Id.* at 56a-57a (citations and brackets omitted). Judge Diaz explained that there is no way to adjudicate petitioner's central contention

---

[2] Judge Motz "concur[red] in Parts I and II.A" of Judge Diaz's lead opinion. Pet. App. 60a. Judge Rushing "agree[d]" with Part II.B.2 and "join[ed]" the conclusion in Part II.C of that opinion. *Id.* at 68a. The introductory paragraph in Part II.B (*id.* at 36a) and Part II.B.1 and II.B.3 of Judge Diaz's opinion (*id.* at 36a-37a, 52a-58a) therefore reflect the views of Judge Diaz only.

that the "NSA is acquiring all communications on a chokepoint cable that it is monitoring" because doing so would "reveal the very information" at the core of the state-secrets assertion: "how Upstream surveillance works and where it's conducted." *Id.* at 57a. And because "'the whole object of [petitioner's] suit' * * * is to inquire into 'the [NSA's] methods and operations'" that are themselves "'state secret[s],'" Judge Diaz concluded that the district court properly dismissed the case without prejudice because petitioner cannot "continue to litigate [its factual allegations] to support standing." *Id.* at 57a-58a.

d. Judge Motz concluded that the panel should not have resolved the merits of any state-secrets issues. Pet. App. 60a-67a. She stated that because this Court had granted certiorari in *Fazaga* to resolve whether Section 1806(f) displaces the state-secrets privilege, she would have stayed the appeal "to await [this] Court's guidance" rather than resolve that issue before *Fazaga* was decided. *Id.* at 60a-61a. Judge Motz further concluded that "judicial restraint similarly counsel[ed] against determining whether the state secrets privilege require[d] dismissal" in this case, *id.* at 61a, observing that only Judge Diaz—and not Judge Rushing—had concluded that the "state secrets doctrine" "require[d] dismissal," *id.* at 62a n.1. Judge Motz stated that she "will not [resolve that issue] here" but "note[d]" her view that Judge Diaz's relevant analysis "raise[d] some serious concerns." *Id.* at 61a-62a; see *id.* at 62a-67a.

ARGUMENT

Petitioner contends (Pet. 20-25, 35) that the state-secrets doctrine is limited to an evidentiary privilege and does not permit dismissal where a plaintiff seeks to prove its case with non-privileged evidence, even

though that evidence would be used to establish a material fact that is a state secret. Alternatively, petitioner contends (Pet. 26-30, 35) that if the doctrine provides for such a dismissal, dismissal would be appropriate here only if the court first concludes, based on its *ex parte*, *in camera* review of the evidence protected by the privilege, that the government has a meritorious "defense" on which the government should prevail if the case were fully adjudicated. Petitioner further contends (Pet. 14, 34-35) that the court of appeals erroneously resolved both of those issues in holding that this case was correctly "dismiss[ed] based on state secrets" grounds. Those contentions lack merit.

The court of appeals did not hold that the state-secrets doctrine required dismissal. Only Judge Diaz reached that conclusion, and petitioner does not contend that a single judge's non-binding views would provide a sound basis for the grant of certiorari. Furthermore, the judgment of the court of appeals is correct and does not conflict with any decision of this Court or any other court of appeals. As a threshold matter, petitioner failed to proffer sufficient evidence at summary judgment to establish the federal courts' Article III jurisdiction. And even if petitioner's evidentiary proffer on Article III standing had been sufficient to survive summary judgment, dismissal was warranted because further adjudication of petitioner's standing would necessarily require the adjudication of factual matters that are themselves state secrets. No further review is warranted.

1. Petitioner seeks certiorari on the premise that the court of appeals held that the state-secrets doctrine required dismissal of this case. More specifically, petitioner asserts that a majority of the appellate panel—

"Judges Diaz and Rushing"—"affirmed the district court's dismissal based on state secrets," Pet. 14, and that the "panel" was "wrong to dismiss [petitioner's] suit on state secrets grounds," Pet. 35. See, *e.g.*, Pet. 3, 26, 34. Petitioner misreads the panel's separate opinions. Only Judge Diaz would have affirmed the grant of summary judgment on state-secrets-dismissal grounds, Pet. App. 52a-58a; his views on that issue did not speak for the court of appeals; and they therefore are not binding on any court in any future case. No sound basis exists to grant certiorari to review Judge Diaz's individual views in this case.

Judge Diaz concluded in Part II.B.3 of his lead opinion that the state-secrets doctrine required dismissal in this case. Pet. App. 52a-58a (Part II.B.3). But no other judge joined that aspect of his opinion. Judge Rushing "agree[d]" only with Part II.B.2 and "join[ed]" the conclusion in Part II.C of the opinion. *Id.* at 68a. Judge Motz, in turn, simply "concur[red] in Parts I and II.A" of the opinion. *Id.* at 60a. The views in Part II.B.3 are therefore those of Judge Diaz alone. See *id.* at 62a n.1 (Motz, J.) (observing that Judge Rushing did "not [conclude that] the state secrets doctrine" "requires dismissal of this case").

Petitioner identifies nothing supporting its assertion (Pet. 14) that Judge Rushing joined Part II.B.3 of Judge Diaz's opinion. Nor would Judge Rushing have had occasion to do so. Judge Rushing specifically determined that petitioner lacked Article III standing because petitioner failed to substantiate standing with sufficient evidence at summary judgment. Pet. App. 68a-72a; cf. *Lujan* v. *Defenders of Wildlife*, 504 U.S. 555, 561(1992). And having concluded that the court lacked Article III jurisdiction to resolve petitioner's case, Judge Rushing

presumably determined that the judicial function ended there. Although a federal court may address whether the state-secrets doctrine requires dismissal as a "'threshold question' * * * *before* addressing jurisdiction," *Tenet* v. *Doe*, 544 U.S. 1, 7 n.4 (2005) (emphasis added), once a court has determined that it lacks Article III jurisdiction, "the only function remaining to the court is that of announcing the fact and dismissing the cause." *Steel Co.* v. *Citizens for a Better Env't*, 523 U.S. 83, 94 (1998) (quoting *Ex parte McCardle*, 74 U.S. (7 Wall.) 506, 514 (1869)). As a result, Judge Rushing "concur[ed]" only "in part" and "in the judgment," Pet. App. 68a, because she agreed that the district court's summary judgment should be affirmed on grounds *different* from those identified by Judge Diaz.

Because Part II.B.3. of Judge Diaz's opinion reflects only Judge Diaz's views on dismissal under the state-secrets doctrine, it does not reflect a determination by the court of appeals, does not constitute precedent, and does not bind any court in any future case. And because the "*court of appeals* has [not] entered a decision" resolving the issue—much less one in conflict with a decision of any other court of appeals—this case does not warrant certiorari. See Sup. Ct. R. 10(a) (emphasis added). Even petitioner does not contend that certiorari would be warranted to consider the non-binding views of a single appellate judge. Such individual views are even less significant than those announced in a panel's unpublished appellate disposition, which (unlike Judge Diaz's state-secrets-dismissal discussion) at least reflects an actual determination by a court of appeals. In the absence of any state-secrets-dismissal holding by the court of appeals in this case, no sound basis exists to grant a writ of certiorari.

2. In any event, certiorari is also unwarranted because the judgment of the court of appeals is correct for reasons independent of the state-secrets doctrine. Petitioner's theory of standing is that the NSA's Upstream surveillance activities copy and review at least some of petitioner's internet communications because, as relevant here, petitioner asserts that the NSA "cop[ies] and review[s] *all* the text-based communications that travel across a given Internet backbone link upon which it conducts Upstream surveillance." Pet. App. 100a (emphasis added); see *id.* at 31a (Diaz, J.); *id.* at 68a (Rushing, J.); see also p. 7-8, *supra*. As Judge Rushing concluded, petitioner failed to offer evidence to substantiate that assertion. Pet. App. 68a-72a.

a. Every trial and appellate judge who has reviewed the voluminous summary-judgment record in this case has concluded that petitioner failed to show that the NSA must necessarily copy and review all internet communications at an Upstream surveillance location. See pp. 8, 10-12, *supra*. And because petitioner ultimately acknowledged that it is "technically feasible to conduct Upstream surveillance *without* copying all communications on a monitored link," petitioner needed to establish instead that the NSA "by choice" has been "copying *all* transactions on a monitored link." Pet. App. 31a (majority opinion) (emphases added). But petitioner submitted no evidence documenting the actual operational details of the NSA's Upstream surveillance activities, and the 2011 FISC opinion on which petitioner relied does not reflect that the NSA was copying "all" such transactions.

The 2011 FISC opinion discussed materially different matters. In that opinion, the FISC reviewed the sufficiency of the government's April 2011 Section

1881a certifications and associated procedures as required by 50 U.S.C. 1881a and concluded that "one aspect of the proposed collection—the 'upstream collection' of Internet transactions containing multiple communications"—was deficient "in some respects." *Redacted*, No. [Redacted], 2011 WL 10945618, at *1 (FISA Ct. Oct. 3, 2011). The court explained that the "NSA's upstream collection devices acquire any Internet transaction transiting the device *if the transaction contains a targeted selector* anywhere within it." *Id.* at *10 (emphasis added); see *id.* at *16 ("NSA's collection devices are set to acquire transactions that contain a reference to the targeted selector."). More specifically, the devices were used to acquire transactions containing "communications to, from, or about a [tasked] selector." *Id.* at *15; see pp. 4-5 & n.1, *supra* (discussing to/from and pre-2018 "about" collection). The problem the FISC identified stemmed in large part from the fact that the internet "'transactions'" that the NSA acquired could not only "contain a single discrete communication"; they could also "contain multiple discrete communications." *Redacted*, 2011 WL 10945618, at *9. The latter transactions are known as multi-communication transactions (MCTs). *Ibid.*

The FISC explained that, "at the time [that an] acquisition" occurred, the "NSA's upstream Internet collection devices [we]re generally incapable of distinguishing between transactions containing only a single discrete communication to, from, or about a tasked selector and transactions containing multiple discrete communications, not all of which may be to, from, or about a tasked selector." *Redacted*, 2011 WL 10945618, at *10. As a result, the "NSA's upstream collection" was acquiring communications that were "*not* to, from, or

about a tasked selector" when such communications were "contained within an MCT that somewhere [in a different communication] reference[d] a tasked selector." *Id.* at *11 (emphasis added). In other words, the NSA was acquiring some number of individual communications that had nothing to do with a tasked selector "by virtue of the fact that [they were] included in *MCTs selected for acquisition* by NSA's upstream collection devices." *Ibid.* (emphasis added). And that problem was exacerbated at the time by "[t]he fact that NSA's technical measures c[ould]not prevent NSA from acquiring transactions containing wholly domestic communications under certain circumstances." *Id.* at *15.

Although the government argued that the Upstream collection of such domestic transactions was "'unintentional'" and reflected merely "a 'failure' of NSA's 'technical means,'" the FISC rejected that position because it found nothing showing that the NSA's devices were "failing to operate as designed." *Redacted*, 2011 WL 10945618, at *15 (citation omitted). Then, in the passage on which petitioner bases its standing theory, the FISC added: "Indeed, the government readily concedes that NSA will acquire a wholly domestic *'about' communication* if the transaction containing the communication is routed through an international Internet link being monitored by NSA or is routed through a foreign server." *Ibid.* (emphasis added).

That statement simply reflected that an "'about'" communication—*i.e.*, a communication "containing a reference to the name of the tasked account," *Redacted*, 2011 WL 10945618, at *5—would be collected because the NSA's collection devices at the time "acquir[ed] communications to, from, or about a [tasked] selector," *id.* at *15, not because the NSA was collecting *every*

transaction that transited an international internet link monitored by the NSA. The FISC understood that the NSA acquired only transactions with communications that contained such a "selector," either because the communication was sent to or from the selector or because the content of the ("about") communication referenced the selector. The FISC demonstrated as much when it concluded its relevant discussion rejecting the government's contention that it unintentionally collected domestic communications by stating that "the Court finds that NSA intentionally acquires Internet *transactions that reference a tasked selector* through its upstream collection with the knowledge that there are tens of thousands of wholly domestic communications contained within those transactions." *Id.* at *16 (emphasis added).

That discussion does not suggest that the NSA's Upstream activities copied every internet transaction that transited a monitored international internet link. In fact, the FISC's repeated focus on the NSA's acquisition of internet transactions containing a tasked selector, to the extent it suggests anything relevant here, suggests that the NSA was *not* acquiring all such transactions.

b. Judge Diaz, joined by Judge Motz, mistakenly viewed the FISC's statement as sufficient to create a genuine issue of material fact based on the view that "reasonable inferences" could be drawn to support an interpretation of the statement as reflecting that "the NSA [wa]s copying all transactions on a monitored link." Pet. App. 31a. That conclusion reflects a misunderstanding of the relevant inquiry.

The proper interpretation of the FISC's 2011 opinion is not a question of fact to be resolved by a trier of fact

based on reasonable inferences. It is a legal question that a court must resolve. For example, "[w]hat issues were decided by [prior] litigation is, of course, a question of law as to which [a] court" is the decisionmaker. *Emich Motors Corp.* v. *General Motors Corp.*, 340 U.S. 558, 571 (1951). This Court has similarly explained that "judges are better suited than are juries to understand and to interpret agency decisions." *Merck Sharp & Dohme Corp.* v. *Albrecht*, 139 S. Ct. 1668, 1680 (2019). And finders of fact would not be permitted to interpret the meaning of statements in opinions of this Court in light of "reasonable inferences" (Pet. App. 31a) that can produce different interpretations depending on which factfinder considers the issue. The same holds true with respect to the 2011 FISC opinion in this case.

Moreover, it is well settled that "general expressions, in every opinion, are to be taken in connection with the case in which those expressions are used." *Landgraf* v. *USI Film Prods.*, 511 U.S. 244, 265 (1994) (quoting *Cohens* v. *Virginia*, 19 U.S. (6 Wheat.) 264, 399 (1821) (Marshall, C.J.)); see *Armour & Co.* v. *Wantock*, 323 U.S. 126, 133 (1944). Judge Diaz's attempt to parse the FISC statement by considering, for instance, its use of the "indefinite article, 'a'" in light of the article's dictionary definition, Pet. App. 33a, thus was misguided. Such language in a court opinion must be "read in context," not "parsed" as if it were the "language of a statute." *Reiter* v. *Sonotone Corp.*, 442 U.S. 330, 341 (1979). And as demonstrated above, the context of the FISC's 2011 opinion shows that the court addressed an issue concerning Upstream surveillance that acquired transmissions to, from, or "about" a selector. The FISC's statement shows nothing more than that the "NSA was collecting communications containing tasked selectors

* * * on the circuits it monitored," not that the "NSA was collecting *all* such communications." Pet. App. 70a (Rushing, J.).

Petitioner therefore failed to proffer sufficient evidence at summary judgment to support its theory of Article III standing. Pet. App. 68a (Rushing, J.). As a result, the judgment of the court of appeals correctly affirmed the grant of summary judgment. And that threshold jurisdictional question presents no issue that might warrant this Court's review.

3. Petitioner contends (Pet. 35-37) that the state-secrets doctrine does not support dismissal in this case, because, in petitioner's view, the doctrine reflects a mere common-law evidentiary privilege. Pet. 15-25. Alternatively, petitioner contends that dismissal would be permitted here only after a court has determined, based on its *ex parte*, *in camera* review of the state-secret information, that the government has asserted a meritorious "defense" on which it would prevail if the case were fully adjudicated, Pet. 25-33. But as explained above, the court of appeals did not render a decision on those matters, and Judge Diaz's individual views do not merit this Court's review. In any event, petitioner's narrow understanding of the state-secrets doctrine is incorrect.

a. From the earliest days of the Republic, courts have recognized the need to protect information critical to national security. See *Martin* v. *Mott*, 25 U.S. (12 Wheat.) 19, 31 (1827); *United States* v. *Burr*, 25 F. Cas. 30, 37 (C.C.D. Va. 1807) (No. 14,692d). This Court's first two detailed discussions of the state-secrets doctrine—*Totten* v. *United States*, 92 U.S. 105, 107 (1876), and *United States* v. *Reynolds*, 345 U.S. 1, 10 (1953)—recognize its importance to the protection of national se-

curity, an interest this Court has repeatedly deemed "compelling." *Department of the Navy* v. *Egan*, 484 U.S. 518, 527 (1988) (citation omitted); see *Haig* v. *Agee*, 453 U.S. 280, 307 (1981). The responsibility to protect national-security information "falls on the President as head of the Executive Branch and as Commander in Chief." *Egan*, 484 U.S. at 527. The state-secrets doctrine accordingly finds its roots not only in "the law of evidence," *Reynolds*, 345 U.S. at 6-7, but also in the Executive's "Art[icle] II dut[y]" to protect "military or diplomatic secrets," *United States* v. *Nixon*, 418 U.S. 683, 710-711 (1974).[3]

The state-secrets doctrine rests on the commonsense principle that, when the national security is at stake, "public policy forbids the maintenance of any suit in a court of justice" that would disclose "matters which the law itself regards as confidential." *Weinberger* v. *Catholic Action of Haw./Peace Educ. Project*, 454 U.S. 139, 146-147 (1981) (*Catholic Action*) (quoting *Totten*, 92 U.S. at 107, and citing *Reynolds*, *supra*); see *Reynolds*, 345 U.S. at 10-11. That doctrine is expressed in two procedural mechanisms, both of which are grounded in the fundamental requirement that the judicial process not jeopardize national security. See *Reynolds*, 345 U.S. at 11 & n.26. First, the doctrine operates through an evidentiary privilege that forecloses reliance on particular evidence protected by the privilege. See *id.* at 7-11. Second, the doctrine requires "dismissal" of an action in appropriate contexts in which resolving the action would otherwise require courts to adjudicate matters that are themselves state secrets and

[3] The government has recently addressed the constitutional basis of the doctrine in this Court. See Pets. Br. at 2-3, 43-45, *FBI* v. *Fazaga*, 142 S. Ct. 1051 (2022) (No. 20-828).

thus "beyond judicial scrutiny." *Catholic Action*, 454 U.S. at 146-147; see, *e.g.*, *Tenet*, 544 U.S. at 7-10. This Court accordingly emphasized last Term that "dismissal pursuant to the state secrets privilege" is "availab[le]" in certain contexts and that the doctrine even "authorizes district courts to dismiss claims on the pleadings." *FBI* v. *Fazaga*, 142 S. Ct. 1051, 1062 (2022).

Petitioner's primary submission is that the state-secrets doctrine generally operates only as an evidentiary privilege and thus does not support dismissal in contexts in which a plaintiff attempts to rely on its own (nonprivileged) evidence to litigate matters that are state secrets. Pet. 15-25. And although petitioner acknowledges (Pet. 21) that *Totten* and *Tenet* directed that cases be dismissed, petitioner argues (*ibid.*) that the principle on which those decisions rest is limited to "disputes over *secret government contracts*." More specifically, petitioner asserts that a state-secrets dismissal "rests on the Court's 'authority to fashion contractual remedies in Government-contracting disputes.'" Pet. 22 (quoting *General Dynamics Corp.* v. *United States*, 563 U.S. 478, 485 (2011)). Petitioner is incorrect.

Petitioner largely bases its position on a passage from *General Dynamics* in which the Court stated that, in that case, it was "called upon to exercise" its "common-law authority to fashion contractual remedies in Government-contracting disputes." *General Dynamics*, 563 U.S. at 485. But the Court in *General Dynamics* did not purport to limit the principle animating *Totten* and *Tenet* to government contract cases. For that reason, the Court had no occasion to discuss other cases that have applied that principle in non-contract contexts. Moreover, this Court in *Tenet* rejected the view that "*Totten* developed merely a contract rule, prohib-

iting breach-of-contact claims seeking to enforce the terms of espionage agreements." *Tenet*, 544 U.S. at 8. And in ruling that "*Totten* was not so limited," the Court determined that *Totten* instead rested on the "more sweeping holding" that "'[p]ublic policy forbids the maintenance of any suit in a court of justice, the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential.'" *Id.* at 8-9 (quoting *Totten*, 92 U.S. at 107).

Catholic Action, for instance, makes clear that dismissal under the state-secrets doctrine is not limited to contract or espionage contexts. As relevant here, the plaintiffs in *Catholic Action* claimed that the United States Navy had violated a provision of the National Environmental Policy Act of 1969 (NEPA), 42 U.S.C. 4321 *et seq.*, under which federal agencies, "'to the fullest extent possible,'" must "prepar[e]" an Environmental Impact Statement (EIS) for any agency recommendations or reports proposing "'major Federal actions significantly affecting the quality of the human environment.'" 454 U.S. at 142 (quoting 42 U.S.C. 4332(2)(C)). The plaintiffs argued that the Navy's decision to construct facilities—which the Navy admitted were "capable of storing nuclear weapons"—at a Navy installation called West Loch to receive "ammunition and weapons" from other Navy installations required that the Navy prepare an EIS because, they argued, an EIS was necessary to account for the "risk of a nuclear accident" and the "effects of radiation from the storage of nuclear weapons in a populated area." *Id.* at 141-142.

This Court reversed the Ninth Circuit's decision and directed that the district court enter a "judgment of dismissal." *Catholic Action*, 454 U.S. at 146-147. The Court observed that an EIS would be required only for

a project that proposed "*stor*[*ing*] nuclear weapons" at the facilities. *Id.* at 146. The Court then explained that "[d]ue to national security reasons, * * * the Navy can neither admit nor deny that it proposes to store nuclear weapons at West Loch" and, for that reason, "it has not been and cannot be established that the Navy has proposed the only action that would require the preparation of an EIS." *Ibid.* Relying on both *Totten* and *Reynolds*, the Court reasoned that it had long "held that 'public policy forbids the maintenance of any suit in a court of justice, the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential, and respecting which it will not allow the confidence to be violated.'" *Id.* at 146-147 (quoting *Totten*, 92 U.S. at 107, and citing *Reynolds*, *supra*). Applying that principle, the Court held that, "[u]ltimately, whether or not the Navy has complied with NEPA 'to the fullest extent possible' is beyond judicial scrutiny." *Id.* at 146. Thus, as this Court has explained, *Catholic Action*'s ruling in a non-contract, non-espionage context applied—and confirmed the "continued vitality" of—*Totten*'s "more sweeping holding" requiring dismissal under the state-secrets doctrine. *Tenet*, 544 U.S. at 9 (discussing *Catholic Action*, *supra*). And as petitioner recognizes (Pet. 17-19), the lower courts have similarly applied the state-secrets doctrine to require dismissal outside government-contract contexts.

b. Petitioner alternatively argues (Pet. 25-33) that if dismissal under the state-secrets doctrine is permitted, dismissal based on a purported "defense" is warranted only after a court has determined based on its *ex parte*, *in camera* review of the state-secrets information that the government has asserted a meritorious "defense"

on which it would prevail if the case were adjudicated on the merits. That too is incorrect.

First, as an initial matter, petitioner's defense-focused arguments rest on a mistaken premise about the nature and procedural posture of this case. The courts of appeals, like Judge Diaz (Pet. App. 54a), have repeatedly recognized that a dismissal on state-secrets grounds is warranted in several distinct contexts, including where (1) the plaintiff is unable to establish the *prima facie* elements of its claim without privileged evidence; (2) the privilege precludes litigation of a "defense to the claim"; and (3) the state-secrets information is so central to the case that "litigating [it] to a judgment on the merits would present an unacceptable risk of disclosing state secrets." *Mohamed* v. *Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1083, 1087 (9th Cir. 2010) (en banc), cert. denied, 563 U.S. 1002 (2011); see, *e.g.*, *In re Sealed Case*, 494 F.3d 139, 145, 148, 153 (D.C. Cir. 2007) (discussing those three contexts, including the final one in which "there is no way [the case] can be litigated without risking national secrets"). Focusing only on the second context, petitioner asserts (Pet. 30-31) that courts of appeals permit dismissal where, based on an *ex parte*, *in camera* review of privileged evidence, the court determines that the government has a meritorious "defense." Petitioner further contends (Pet. 26-28) that the courts of appeals are divided on that issue.

But the threshold state-secrets issue in this case does not pertain to a government "defense"; it concerns *petitioner's* burden to establish its own Article III standing by showing that at least some of petitioner's communications were copied and reviewed as part of the NSA's Upstream surveillance activities. And it is petitioner's affirmative showing on standing—not a de-

fense on which the government has the burden of proof —that would unavoidably require adjudication of matters that are state secrets. For that reason, Judge Diaz concluded that he did not need to decide if a "putative defense is 'valid' " in order to warrant dismissal, because dismissal is warranted in this case for the independent reason that " 'state secrets are so central to [this] proceeding that it cannot be litigated without threatening their disclosure.' " Pet. App. 56a-57a (citation omitted). In short, this case does not present the defense-focused question on which petitioner seeks review and thus does not implicate petitioner's asserted division of authority.

In any event, petitioner's defense-focused contentions misapprehend the nature of a state-secrets dismissal. A dismissal under the state-secrets doctrine is not a dismissal on the merits, reflecting that one side or the other should have prevailed if privileged evidence had been available to fully adjudicate the case. It is a dismissal reflecting that the relevant claim is "beyond judicial scrutiny" because its full adjudication " 'would inevitably lead to the disclosure of matters which the law itself regards as confidential.' " *Catholic Action*, 454 U.S. at 146-147 (quoting *Totten*, 92 U.S. at 107).

This Court has thus emphasized that if a court can determine, based on the government's submissions, that the government has properly asserted the state-secrets privilege—*i.e.*, the court finds a reasonable danger exists that disclosing the evidence in question would expose information "that 'should not be divulged' in 'the interest of national security' "—the court should not jeopardize the security of that information by conducting "even *in camera*, *ex parte* review of the relevant evidence." *Fazaga*, 142 S. Ct. at 1062 (quoting *Reynolds*, 345 U.S. 10). Petitioner's position would turn that prin-

ciple on its head. It makes little sense in this context, where the doctrine's polestar is the protection of national security, to require a court to conduct a shadow adjudication and reach a merits conclusion in order to dismiss a case as nonjusticiable. If that were the rule, dismissals based on a nominally nondisclosed court ruling would often risk revealing the very information that the state-secrets doctrine is designed to protect. See *Clapper* v. *Amnesty Int'l USA*, 568 U.S. 398, 412 n.4 (2013) (rejecting the argument that the government should be required to disclose *in camera* whether it was surveilling plaintiffs under Section 1881a because it was the "[plaintiffs'] burden to prove their standing" and because such an adjudication would disclose the scope of the United States' foreign-intelligence surveillance through, *inter alia*, the court's "postdisclosure decision about whether to dismiss the suit for lack of standing," which "would surely signal to the terrorist whether his name was on the list of surveillance targets").

In this case, for instance, petitioner's standing theory depends on its view that the NSA is "copying all [internet] transactions on a monitored [international internet] link." Pet. App. 31a (majority opinion); see pp. 7-8, 17, *supra*. As Judge Diaz recognized—and as petitioner does not appear to dispute—litigating whether that assertion is correct in order to "support [petitioner's] standing" would depend on establishing "how Upstream surveillance works," such that the "'whole object'" of petitioner's position is to "inquire into 'the methods and operations of the NSA'"—matters that the courts below found (and petitioner does not dispute) are state secrets. Pet. App. 57a-58a (citation and brackets omitted). If a court were either to dismiss or decline to dismiss based on its resolution of petitioner's factual asser-

tion after reviewing the government's privileged (and highly classified) evidence on the matter, the dismissal would effectively reveal sensitive intelligence matters—state secrets—that cannot be publicly confirmed or denied without significant harm to the national security.

Finally, petitioner fails to account for the fact that the state-secrets doctrine is not limited to cases like this in which the government is the defendant. The government may, for instance, invoke the doctrine in litigation between private parties in order to protect the national security. See, *e.g.*, *United States* v. *Zubaydah*, 142 S. Ct. 959, 968, 970-971 (2022); *Mohamed*, 614 F.3d at 1087-1090 (en banc holding that dismissal was warranted in a suit between private parties where state secrets pervaded "the claims and possible defenses"); *Bareford* v. *General Dynamics Corp.*, 973 F.2d 1138, 1143-1144 (5th Cir. 1992) (affirming dismissal of an action between private parties where privileged information was "central 'to the very question upon which a decision must be rendered'") (citation omitted), cert. denied, 507 U.S. 1029 (1993); *Fitzgerald* v. *Penthouse Int'l, Ltd.*, 776 F.2d 1236, 1243-1244 (4th Cir. 1985) (same; explaining that the "case could [not] be tried without compromising sensitive military secrets"). And if the government is not a party, petitioner offers no sound reason why the government's ability to protect the national security in such a suit should depend on whether a non-government defendant should prevail on the merits.

CONCLUSION

The petition for a writ of certiorari should be denied.

Respectfully submitted.

ELIZABETH B. PRELOGAR
Solicitor General
BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General
SHARON SWINGLE
JOSEPH F. BUSA
Attorneys

JANUARY 2023