PUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 20-1191

WIKIMEDIA FOUNDATION,

Plaintiff − Appellant,

and

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

Plaintiffs,

v.

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE; GENERAL 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; RICHARD GRENELL, in his official capacity as acting Director of National Intelligence; MERRICK B. GARLAND, Attorney General; DEPARTMENT OF JUSTICE,

Defendants – Appellees.

CENTER FOR DEMOCRACY & TECHNOLOGY; NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE; DAVID H. KAYE, Evidence Law Professor; EDWARD J. IMWINKELRIED, Evidence Law Professor; D. MICHAEL RISINGER, Evidence Law Professor; REBECCA WEXLER, Evidence Law Professor; PROFESSOR STEPHEN I. VLADECK; AMERICANS FOR PROSPERITY FOUNDATION; BRENNAN CENTER FOR JUSTICE; ELECTRONIC FRONTIER FOUNDATION; ELECTRONIC PRIVACY INFORMATION CENTER; FREEDOMWORKS FOUNDATION; TECHFREEDOM; NETWORK ENGINEERS AND TECHNOLOGISTS,

Amici Supporting Appellant.

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

Argued: March 12, 2021 Decided: September 15, 2021

Before MOTZ, DIAZ, and RUSHING, Circuit Judges.

Affirmed by published opinion. Judge Diaz wrote the majority opinion, in which Judge Motz joined as to Parts I and II.A, and in which Judge Rushing joined as to Part II.B.2 and C. Judge Motz wrote an opinion concurring in part and dissenting in part. Judge Rushing wrote an opinion concurring in part and in the judgment.

ARGUED: Patrick Christopher Toomey, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, New York, New York, for Appellant. Joseph Forrest Busa, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C., for Appellees. **ON BRIEF:** Deborah A. Jeon, David R. Rocah, AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND, Baltimore, Maryland; Ashley Gorski, Charles Hogle, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, New York, New York; Benjamin H. Kleine, COOLEY LLP, San Francisco, California; Alex Abdo, Jameel Jaffer, KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY, New York, New York, for Appellant. Ethan P. Davis, Acting Assistant Attorney General, H. Thomas Byron III, Civil Division, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C., for Appellees. Avery W. Gardiner, Gregory T. Nojeim, Mana Azarmi, Stan Adams, CENTER FOR DEMOCRACY & TECHNOLOGY, Washington, D.C.; Sharon Bradford Franklin, Ross Schulman, NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE, Washington, D.C.; Andrew A. Bank, Bret S. Cohen, Allison M. Holt Ryan, Stevie N. DeGroff, HOGAN LOVELS US LLP, Washington, D.C., for Amici Center for Democracy & Technology and New America's Open Technology Institute. Benjamin B. Au, W. Henry Huttinger, Los Angeles, California, Aditya V. Kamdar, DURIE TANGRI LLP, San Francisco, California, for Amici Evidence Law Professors. Lauren Gallo White, San Francisco, California, Brian M. Willen, WILSON SONSINI GOODRICH & ROSATI PROFESSIONAL CORPORATION, New York, New York, for Amicus Professor Stephen I. Vladeck. Eric R. Bolinder, AMERICANS FOR PROSPERITY FOUNDATION, Arlington, Virginia; Sophia Cope, Mark Rumold, Andrew Cocker, ELECTRONIC FRONTIER FOUNDATION, San Francisco, California, for Amici

Americans for Prosperity Foundation, Brennan Center for Justice, Electronic Frontier Foundation, Electronic Privacy Information Center, FreedomWorks Foundation, and TechFreedom. Jonathan Blavin, Elizabeth Kim, Alexander Gorin, MUNGER, TOLLES & OLSON LLP, San Francisco, California, for Amici Network Engineers and Technologists.

DIAZ, Circuit Judge:

We consider, for the second time, the Wikimedia Foundation's contentions that the government is spying on its communications using Upstream, an electronic surveillance program run by the National Security Agency ("NSA"). In the first appeal, we found Wikimedia's allegations of Article III standing sufficient to survive a motion to dismiss and vacated the district court's judgment to the contrary. On remand, the court again dismissed the case, holding that Wikimedia didn't establish a genuine issue of material fact as to standing and that further litigation would unjustifiably risk the disclosure of state secrets.

Although the district court erred in granting summary judgment to the government as to Wikimedia's standing, we agree that the state secrets privilege requires the termination of this suit. We thus affirm.

I.

Our prior opinion contains many of the relevant facts, including descriptions of the Upstream surveillance program and its authorizing statute, Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1881a. *See Wikimedia Found. v. Nat'l Sec. Agency/Cent. Sec. Serv.*, 857 F.3d 193, 200–07 (4th Cir. 2017). We take a moment here to briefly review the inner workings of Upstream, recap our previous decision, and relate what has occurred since then.

A.

As its name suggests, Upstream surveillance involves the NSA's collection of communications on the Internet backbone, "upstream" of the Internet user, by compelling the assistance of telecommunications-service providers. By contrast, the NSA obtains the "vast majority" of Internet communications collected under Section 702 directly from a user's Internet-service provider through the PRISM surveillance program, *Redacted*, 2011 WL 10945618, at *9 & n.23 (FISA Ct. Oct. 3, 2011), which isn't at issue here.

The Internet backbone consists of domestic "high-speed, ultra-high bandwidth data-transmission lines" and the relatively limited number of submarine and terrestrial circuits that carry Internet communications into and out of the United States, J.A. 2739, which are often referred to as "chokepoint" cables. More specifically:

> The NSA performs Upstream surveillance by first identifying a target and then identifying "selectors" for that target. Selectors are the specific means by which the target communicates, such as e-mail addresses or telephone numbers. Selectors cannot be keywords (e.g., "bomb") or names of targeted individuals (e.g., "Bin Laden").
>
> The NSA then "tasks" selectors for collection and sends them to telecommunications-service providers. Those providers must assist the government in intercepting communications to, from, or "about" the selectors. "About" communications are those that contain a tasked selector in their content, but are not to or from the target.

Wikimedia Found., 857 F.3d at 202.[1]

[1] The NSA suspended its collection of "about" communications in 2017 but continues to collect "to" and "from" communications.

Importantly, "[w]hile Upstream surveillance is intended to acquire Internet *communications*, it does so through the acquisition of Internet *transactions*." *Id.* at 203 (cleaned up). When an individual sends a communication over the Internet, it's broken up into one or more data packets that are transmitted to, and reassembled by, the receiving device. Each packet travels separately across the Internet backbone. This means that packets may take different paths to the recipient, and while in transit, they're mixed with countless other packets making their own journeys.

"[A] complement of packets traversing the Internet that together may be understood by a device on the Internet" as one or many discrete communications comprises an Internet "transaction." *Redacted*, 2011 WL 10945618, at *9 n.23 (quoting a government submission to the Foreign Intelligence Surveillance Court ("FISC")). "If a single discrete communication within [a 'multi-communication transaction'] is to, from, or [until 2017] about, a Section 702-tasked selector, and at least one end of the transaction is foreign, the NSA will acquire the entire [multi-communication transaction]." Privacy & Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 44 (2014) ("PCLOB Report").

B.

Wikimedia and eight other plaintiffs sued the government, seeking "among other things, a declaration that Upstream surveillance violates the First and Fourth Amendments, an order permanently enjoining the NSA from conducting Upstream surveillance, and an order directing the NSA to purge all records of Plaintiffs' communications" obtained

through Upstream surveillance. *Wikimedia Found.*, 857 F.3d at 202 (cleaned up). The district court dismissed the case for lack of Article III standing, and the plaintiffs appealed.

Article III "[s]tanding is part and parcel of the constitutional mandate that the judicial power of the United States extend only to 'cases' and 'controversies.'" *Libertarian Party of Va. v. Judd*, 718 F.3d 308, 313 (4th Cir. 2013) (quoting U.S. Const. art. III, § 2). To establish standing, a plaintiff must show: "(1) an injury in fact, (2) a sufficient causal connection between the injury and the conduct complained of, and (3) a likelihood that the injury will be redressed by a favorable decision." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 157–58 (2014) (cleaned up).

In what we called the "Wikimedia Allegation," Wikimedia claimed it had standing because (1) its communications travel across every international Internet link[2]; (2) the NSA conducts Upstream surveillance on at least one such link; and (3) "in order for the NSA to reliably obtain communications to, from, or about its targets in the way it has described, the government must be copying and reviewing all the international text-based communications that travel across a given link." J.A. 57.

Together, these assertions were "sufficient to make plausible the conclusion that the NSA is intercepting, copying, and reviewing at least some of Wikimedia's communications," establishing an injury-in-fact for a Fourth Amendment violation. *Wikimedia Found.*, 857 F.3d at 211. "And, because Wikimedia has self-censored its speech

[2] Wikimedia uses "international" to describe something occurring between the United States and a foreign country and "international Internet link" to mean a chokepoint cable.

and sometimes forgone electronic communications" as a result of that surveillance, it established an injury-in-fact for purposes of its First Amendment claim. *Id.* Wikimedia also met the two other requirements for standing because "Upstream surveillance is the direct cause of the alleged injury, and there's no reason to doubt that the requested injunctive and declaratory relief would redress the harm." *Id.* at 210.

We thus vacated the district court's judgment as to Wikimedia. We affirmed as to the other eight plaintiffs, who alleged that given the government's incentives to cast a wide net, "the NSA is intercepting, copying, and reviewing substantially all text-based communications entering and leaving the United States, including their own." *Wikimedia Found.*, 857 F.3d at 202 (cleaned up). We concluded that such claims "about what the NSA 'must' be doing" based on its goals "lack sufficient factual support to get 'across the line from conceivable to plausible.'" *Id.* at 214 (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)).

C.

On remand, the district court ordered jurisdictional discovery. But when Wikimedia sought evidence related to Upstream, the NSA invoked the state secrets privilege.

The privilege permits the United States to "prevent the disclosure of information in a judicial proceeding if 'there is a reasonable danger' that such disclosure 'will expose [matters of state] which, in the interest of national security, should not be divulged.'" *El-Masri v. United States*, 479 F.3d 296, 302 (4th Cir. 2007) (quoting *United States v. Reynolds*, 345 U.S. 1, 10 (1953)). In *Reynolds,* the decision that modernized the privilege, three civilian observers aboard an Air Force bomber testing secret electronic equipment

died when the plane caught fire and crashed. 345 U.S. at 3. Their widows sued the United States under the Federal Tort Claims Act and sought discovery related to the incident. *Id.* at 3, 6. Instead of producing the requested information, the Secretary of the Air Force filed a formal claim of privilege, citing national security concerns. *Id.* at 4–5. The Supreme Court concluded that the government properly invoked the privilege and sustained its refusal to disclose the documents at issue. *Id.* at 6.

Thus, to invoke the state secrets privilege, the United States must make "a formal claim of privilege, lodged by the head of the department which has control over the matter, after actual personal consideration by that officer." *Id.* at 7–8. Here, the government filed the declaration of Daniel Coats, the then Director of National Intelligence, who attested that the disclosures requested by Wikimedia "reasonably could be expected to cause serious damage, and in many cases exceptionally grave damage, to the national security of the United States."[3] J.A. 174.

In particular, Director Coats asserted the privilege over seven categories of information:

> (A) information that would tend to confirm what individuals or entities are subject to Upstream surveillance activities; (B) information concerning the operational details of the Upstream collection process; (C) the location(s) at which Upstream surveillance is conducted; (D) the categories of Internet-based communications collected through Upstream surveillance activities; (E) information concerning the scope and scale of Upstream surveillance; (F) NSA cryptanalytic capabilities; and (G) additional categories of classified

[3] The government also filed the classified declaration of George Barnes, the then Deputy Director of the NSA, describing the national security concerns in greater detail.

> information regarding Upstream surveillance contained in opinions and orders issued by, and submissions made to, the [FISC].

J.A. 174–75.

Director Coats also confirmed several key facts about Upstream surveillance. He explained that "in the course of the Upstream collection process, certain Internet transactions transiting the Internet backbone network(s) of certain electronic communication service provider(s) are filtered for the purpose of excluding wholly domestic communications." J.A. 177. The NSA then scans the remaining communications "to identify for acquisition those transactions that are to or from" (or, until 2017, "about") the targeted selector and "ingest[s]" them into government databases. J.A. 177–78.

Director Coats further acknowledged that the NSA "is monitoring at least one circuit carrying international Internet communications." J.A. 186. But he maintained that "[w]hile the Upstream collection process has been described in general terms in this declaration and in declassified documents and unclassified reports, certain operational details of Upstream collection remain highly classified." J.A. 178.

Despite the NSA's claim of privilege, Wikimedia moved to compel discovery. Wikimedia argued that FISA's discovery procedures, as provided in 50 U.S.C. § 1806(f), displace the state secrets privilege in cases involving government-run electronic surveillance. This provision permits an "aggrieved person" who is the target of electronic surveillance to request, under certain circumstances, that the court conduct an in camera and ex parte review of "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." 50 U.S.C. § 1806(f). Wikimedia contended that (1) it had successfully alleged that it was an aggrieved person; and (2) § 1806(f) required the district court to review evidence related to Upstream surveillance in camera and ex parte to determine whether the NSA lawfully surveilled Wikimedia's communications, instead of dismissing the entire action.

The district court, however, concluded that FISA doesn't apply and denied Wikimedia's motion. In particular, the court explained that the "§ 1806(f) procedures do not apply where, as here, a plaintiff has not yet established that it has been the subject of electronic surveillance." *Wikimedia Found. v. Nat'l Sec. Agency/Cent. Sec. Serv.*, 335 F. Supp. 3d 772, 780 (D. Md. 2018). Because Wikimedia had "merely plausibly alleged that it has been the target of surveillance and ha[d] not yet adduced evidence establishing this fact of surveillance," the court determined that "it [wa]s not appropriate . . . to engage in *ex parte* and *in camera* review of the materials responsive to plaintiff's interrogatories or to those plaintiff describe[d] in its motion to compel." *Id.* at 786.

D.

The government then moved for summary judgment, contending that Wikimedia didn't establish a genuine issue of material fact as to the second or third prongs of the Wikimedia Allegation[4] and that the state secrets privilege independently requires dismissal of the case. As we explain in further detail below, the district court granted this motion, holding that (1) Wikimedia established a genuine issue of material fact as to the second but

[4] The government didn't dispute that Wikimedia had established the first prong.

not the third prong of the Wikimedia Allegation,[5] (2) the state secrets privilege foreclosed further litigation, and (3) Wikimedia didn't show any other injury that gives rise to standing.

1.

The district court first determined that Wikimedia had established a genuine issue of material fact as to the second prong of the Wikimedia Allegation, which posits that the NSA conducts Upstream surveillance on at least one international Internet link.

To prove this assertion, Wikimedia primarily relied on a declassified 2011 FISC opinion, which states that "the government readily concedes that [the] NSA will acquire a wholly domestic 'about' communication if the transaction containing the communication is routed through an international Internet link being monitored by [the] NSA or is routed through a foreign server." *Redacted*, 2011 WL 10945618, at *15 (citing a government submission to the FISC). An NSA witness confirmed the accuracy of this sentence, and of the opinion generally, as of October 2011.[6]

[5] The district court held that Wikimedia "established" the second prong of the Wikimedia Allegation "without a genuine dispute as to any material fact." *Wikimedia Found. v. Nat'l Sec. Agency/Cent. Sec. Serv.*, 427 F. Supp. 3d 582, 603 (D. Md. 2019). Read literally, the court appears to have granted partial summary judgment for Wikimedia on the second prong. But, although Wikimedia opposed the government's summary judgment motion, it never filed its own motion. Nor did the court invoke Federal Rule of Civil Procedure 56(f), which allows it to grant summary judgment to a nonmovant under certain circumstances. To square this circle, we assume that the district court found only that Wikimedia established a genuine issue of material fact on the second prong.

[6] The district court recognized the quoted sentence as an admissible statement by a party opponent. *See Wikimedia Found.*, 427 F. Supp. 3d at 602. On appeal, Wikimedia

But the government contended that the meaning of the phrase "international Internet link" as used in the FISC opinion isn't the same as that used in the Wikimedia Allegation. In fact, the NSA witness testified that the "NSA has an understanding of this term that is specific to how [the FISC] described it," but that its true definition can't be confirmed or denied because "it's classified." J.A. 447. And the government pointed out that the 2011 FISC opinion may not reflect the NSA's current practices.

"Rather than belabor the squabble between the parties about the meaning of this particular term" in the FISC opinion, the district court zeroed in on an entirely different government disclosure. *Wikimedia Found.*, 427 F. Supp. 3d at 602–03. The court sua sponte relied on Director Coats's statement that the "NSA is monitoring at least one circuit carrying international Internet communications" to conclude that Wikimedia had produced sufficient evidence to raise a genuine issue of material fact as to the second prong of the Wikimedia Allegation (i.e., that the NSA conducts Upstream surveillance on at least one international Internet link). *Id.* at 603.

2.

But the district court found that Wikimedia didn't establish a genuine issue of material fact as to the third prong of the Wikimedia Allegation, which asserts that the NSA is copying all communications on a monitored link. At the motion-to-dismiss stage, Wikimedia had alleged that "as a technical matter, the government cannot know

---

asserts, and the government doesn't dispute, that the NSA also adopted the facts in the FISC opinion as a whole.

beforehand which communications will contain selectors associated with its targets, and therefore it must copy and review all international text-based communications transiting a circuit in order to identify those of interest." *Wikimedia Found.*, 857 F.3d at 204 (cleaned up).

To undermine that claim, the government offered the declarations of Henning Schulzrinne, an "expert in internet technology." Appellee's Br. at 44. Schulzrinne wasn't privy to any classified or other non-public information about how the NSA actually operates Upstream surveillance, so he instead opined that the NSA could "in theory" use a technique called traffic mirroring to conduct Upstream-style surveillance without copying Wikimedia's communications. J.A. 719.

According to Schulzrinne, traffic mirroring requires installing a link (i.e., a fiber-optic cable) between the surveilling entity's equipment and a mirror port on the router or switch directing Internet traffic at the target location. The router or switch is then configured to copy traffic from one link to another without interrupting the original. It can also be programmed to whitelist or blacklist certain IP addresses, thereby filtering the data before copying it. Whitelisting involves copying only communications from specific IP addresses, while blacklisting involves copying everything except communications from specific IP addresses.

Wikimedia responded with the declarations of Scott Bradner, "an Internet networking expert." Appellant's Br. at 23. Although Bradner conceded that it's "technically possible" to use traffic mirroring with filtering (as envisioned by Schulzrinne),

"doing so would purposefully ignore most of the Internet" and "would be inconsistent with the publicly known details about the [U]pstream collection program." J.A. 3898.

Bradner explained that traffic mirroring with filtering "would require either that the [Internet Service Provider ("ISP")] agree to place an NSA-operated device into the heart of its network"—which could negatively impact "the ISP's network in the event of an equipment failure or misconfiguration—or that the ISP's personnel have enough knowledge of the filter criteria to configure the ISP's router." J.A. 1023. Moreover, these filters would "place potentially significant additional demands on the router's processing power, which could affect the performance of the router and create a risk of overloading the router, thereby interfering with the ISP's ability to support its customers' traffic." J.A. 1025.

Bradner further opined that rather than traffic mirroring with filtering, the NSA is "most likely" using link-layer copying (essentially traffic mirroring without filtering) or optical splitters. J.A. 1022. An optical splitter is a physical device attached to a fiber-optic cable that reflects a portion of the light traveling down that circuit to a different receiver. The information continues on its original course, while an exact duplicate is sent to the surveilling entity. Any filtering must take place after the copy is made. The technology is "extremely reliable as it consumes no power, has no software, and cannot slow traffic." Technologists' Amicus Br. at 10; *see also* J.A. 3921. According to Bradner, link-layer copying and optical splitters offer the NSA the "greatest operational control and confidentiality in carrying out upstream collection with the least risk of interference with the ISP's ordinary network operations." J.A. 1025.

Bradner also pointed to several government disclosures as evidence that the NSA is copying all communications on a monitored link. These include the previously discussed statement from the 2011 FISC opinion, which provides that the "NSA will acquire a wholly domestic 'about' communication if the transaction containing the communication is routed through an international Internet link being monitored by [the] NSA or is routed through a foreign server," *Redacted*, 2011 WL 10945618, at *15; and a government report stating that the NSA's goal is to "comprehensively acquire communications that are sent to or from its targets," PCLOB Report 10, 37, 123.[7]

Of these disclosures, the district court mentioned only the PCLOB Report in the context of Bradner's opinion that the NSA is likely conducting Upstream surveillance using link-layer copying or optical splitters rather than traffic mirroring with filtering. *See Wikimedia Found.*, 427 F. Supp. 3d at 603–10. It declined to consider this opinion, reasoning that it rests on "speculative assumptions about the NSA's surveillance practices

[7] Wikimedia's evidence also included (1) another government report revealing that the NSA had more than 120,000 Section 702 targets in 2017, Office of the Director of National Intelligence Statistical Transparency Report for 2017 (Apr. 2018); (2) "[t]he leading treatise on national security investigations, co-authored by the former Assistant Attorney General for National Security," Appellant's Br. at 31–32 (citing David Kris & J. Douglas Wilson, Nat'l Security Investigations & Prosecutions 2d § 17.5 (2015)); (3) "[r]ecent disclosures by the United Kingdom about functionally equivalent surveillance undertaken by the NSA's British counterpart," *id.* at 32 (citing Further Observations of the Government of the United Kingdom, Human Rights Organizations v. United Kingdom, Eur. Ct. H.R. (Dec. 16, 2016), https://privacyinternational.org/sites/default/files/2018-02/2016.12.16%20Government%27s%20further%20obs.pdf); and (4) descriptions of "the U.S. government's EINSTEIN 2 surveillance program, which protects government networks through a similar form of Internet surveillance," *id.* (citing Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (EINSTEIN 2.0), 33 Op. O.L.C. 1 (Jan. 9, 2009)).

and priorities and [its] resources and capabilities." *Id.* at 604–05 (citing Fed. R. of Evid. 702 and *Daubert v. Merrell Dow Pharms., Inc.*, 509 U.S. 579 (1993)).

The court instead focused on the technical arguments presented by both sides and concluded that the record didn't establish that the NSA must copy all communications on a surveilled circuit by "technological necessity." *Id.* at 609. It therefore held that Wikimedia had failed to establish a genuine issue for trial as to standing.

3.

The district court next "assum[ed] *arguendo* that[] there is a genuine dispute of material fact as to the third prong of the Wikimedia Allegation," yet still determined that the case must be dismissed because of the state secrets privilege. *Id.* at 610.

In doing so, the court again rejected Wikimedia's argument that FISA displaces the state secrets privilege in this case. This time, it distinguished Wikimedia's case from the only other circuit case directly addressing this issue, *Fazaga v. FBI*, 916 F.3d 1202 (9th Cir. 2019), *amended on denial of reh'g en banc by* 965 F.3d 1015 (9th Cir. 2020), *cert. granted*, 2021 WL 2301971 (June 7, 2021), which holds that FISA's discovery procedures in § 1806(f) apply instead of the state secrets privilege under certain circumstances.

The plaintiffs there challenged a counter-terrorism investigation involving electronic surveillance conducted by an informant for the Federal Bureau of Investigation. "Several sources," including the Bureau, had confirmed the identity of the informant and that he "created audio and video recordings" for the investigation. *Fazaga*, 965 F.3d at 1028.

The *Fazaga* district court dismissed all but one of the plaintiffs' claims at the pleading stage based on the government's assertion of the state secrets privilege. But the Ninth Circuit reversed, holding that FISA displaces the privilege whenever "an aggrieved person affirmatively challenges, in any civil case, the legality of electronic surveillance or its use in litigation, whether the challenge is under FISA itself, the Constitution, or any other law" and that "[t]he complaint's allegations are sufficient if proven to establish that Plaintiffs are 'aggrieved persons'" who had been subjected to electronic surveillance by the government. *Id.* at 1030, 1053.

The district court here determined that even if *Fazaga* were binding in our circuit such that § 1806(f) displaces the state secrets privilege, it wouldn't help Wikimedia. That's because the Ninth Circuit found the *Fazaga* plaintiffs' allegations sufficient to establish that they were aggrieved persons (as required to apply § 1806(f)) at the motion-to-dismiss stage. Wikimedia, on the other hand, faced summary judgment and thus needed to establish a genuine issue of material fact that it was the subject of electronic surveillance but had failed to do so. Accordingly, the court concluded once more that the § 1806(f) procedures don't apply.

That being so, the court turned to the government's claim of privilege. It determined that state secrets are "so central" to litigating the Wikimedia Allegation that "the defendants cannot properly defend themselves without using privileged evidence," *Wikimedia Found.*, 427 F. Supp. 3d at 613, and that further proceedings "would present an unjustifiable risk" of disclosing privileged information, *id.* at 612. The court thus ruled that the case must also be dismissed because of the state secrets privilege.

4.

Finally, the district court concluded that none of Wikimedia's other alleged injuries independently establish standing. In addition to the Wikimedia Allegation, Wikimedia asserted that: (1) Upstream surveillance impaired Wikimedia's communications with its community members, as evidenced by the drop in readership for certain Wikipedia pages; (2) Wikimedia had to take costly protective measures against Upstream surveillance; and (3) Wikimedia has third party standing to assert its users' rights. The court held that the first two theories fail under *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), and the last collapses under its own weight.

In *Clapper*, several plaintiffs in the United States challenged Section 702, alleging that their work "requires them to engage in sensitive international communications with individuals who they believe are likely targets of surveillance." 568 U.S. at 401. As we described in our prior opinion, the plaintiffs there "had two separate theories of Article III standing: (1) there was an 'objectively reasonable likelihood' that their communications would be intercepted in the future pursuant to Section 702 surveillance, and (2) they were forced to undertake costly and burdensome measures to avoid a substantial risk of surveillance." *Wikimedia Found.*, 857 F.3d at 206 (quoting *Clapper*, 568 U.S. at 407). "They did not, however, have actual knowledge of the Government's Section 702 targeting practices." *Id.* (cleaned up). The Supreme Court held that neither theory was sufficient to prove standing at the summary-judgment stage because they depended on a "speculative chain of possibilities [that] does not establish that injury based on potential future

surveillance is certainly impending or is fairly traceable" to Section 702 surveillance. *Clapper*, 568 U.S. at 414.

As relevant to Wikimedia's claim of decreased readership, *Clapper* explained that "a chilling effect arising merely from the individual's knowledge that a governmental agency was engaged in certain activities or from the individual's concomitant fear that, armed with the fruits of those activities, the agency might in the future take some other and additional action detrimental to that individual" doesn't establish standing. 568 U.S. at 417–18; *see also id.* at 418 ("Because allegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm, the plaintiffs . . . lack standing." (cleaned up)).

The district court found that Wikimedia made a similarly deficient assertion: that its "decreased readership is a result of individual[] fear that the government might be monitoring their Internet activity and might use that information at some later date." *Wikimedia Found.*, 427 F. Supp. 3d at 616. The court then determined that Wikimedia otherwise lacked objective evidence of "an ongoing and sustained drop in [its] readership," or that any such decline stemmed from "Upstream surveillance specifically" rather than "media coverage of NSA surveillance generally." *Id.* (cleaned up). It thus concluded that Wikimedia's reduction in readership didn't establish standing.

In assessing Wikimedia's standing based on protective measures, the district court pointed to *Clapper*'s admonition that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm." 568 U.S. at 416. By finding the summary judgment record inadequate to establish the Wikimedia

Allegation, the court had already ruled that any harm to Wikimedia from Upstream surveillance was "purely hypothetical" and thus insufficient to prove standing. *Wikimedia Found.*, 427 F. Supp. 3d at 617. As an additional nail in the coffin, the court observed that Wikimedia began implementing its protective measures years before learning about Upstream for a variety of other reasons, "including protecting against individual computer hackers and keeping . . . company policies up-to-date and transparent," so the requested injunctive and declaratory relief "would not redress any alleged injury from these protective expenditures." *Id.* at 617 n.63.

Nor was the district court persuaded that Wikimedia had established third party standing. For third party standing, a plaintiff must demonstrate "(1) an injury-in-fact; (2) a close relationship between [itself] and the person whose right [it] seeks to assert; and (3) a hindrance to the third party's ability to protect his or her own interests." *Freilich v. Upper Chesapeake Health Inc.*, 313 F.3d 205, 215 (4th Cir. 2002).

The court held that Wikimedia didn't satisfy any of these elements. As discussed, the court had already rejected all of Wikimedia's alleged injuries-in-fact. The court also determined that, unlike lawyers and clients or doctors and patients, Wikimedia doesn't have the requisite "protected, close relationships" with its "largely unidentified contributors." *Wikimedia Found.*, 427 F. Supp. 3d at 617 & n.65. In fact, Wikimedia "only presented declarations from one single contributor," who claimed that the "normal burdens of litigation" and her "workload as a medical student" make it "impossible" for her to bring suit. *Id.* at 617–18. The court found this "insufficient" to show that an obstacle prevents her from protecting her own interests. *Id.* at 618.

The district court thus dispatched all of Wikimedia's theories of standing, dismissed the case, and entered judgment for the government. This appeal followed.

II.

Wikimedia contends that the district court erred in dismissing its case because (1) the evidence it presented establishes a genuine dispute of material fact with respect to its standing; (2) FISA displaces the state secrets privilege in this context; (3) even if FISA doesn't apply, the state secrets privilege doesn't require dismissal because "Wikimedia can establish its standing without resort to privileged evidence[]" and the government hasn't shown that it can't defend itself without privileged evidence; and (4) "Wikimedia has presented evidence of additional injuries" that don't implicate any state secrets. Appellant's Br. at 14, 17.

As we explain, the record evidence is sufficient to establish a genuine issue of material fact as to Wikimedia's standing. But FISA doesn't displace the state secrets privilege, and further litigation would unjustifiably risk the disclosure of privileged information. And because Wikimedia's other alleged injuries don't provide independent bases for standing, this case must be dismissed.

A.

Because standing is jurisdictional, we begin our discussion there. *See Libertarian Party of Va.*, 718 F.3d at 313. Our review of a district court's decision on summary judgment is de novo, and we view all facts and reasonable inferences in the light most

favorable to the nonmovant—here, Wikimedia. *See Sylvia Dev. Corp. v. Calvert Cnty.*, 48 F.3d 810, 817 (4th Cir. 1995).

1.

The government maintains that Wikimedia hasn't established a genuine issue for trial as to standing on the second prong of the Wikimedia Allegation: that Upstream surveillance occurs on at least one international Internet link. We disagree.

Wikimedia contends that an "international Internet link" is a "chokepoint" cable, which refers to one of the relatively limited number of circuits that carry Internet communications into and out of the United States. Because Wikimedia claims that its communications traverse all chokepoint cables—but not necessarily all other circuits on the Internet backbone—the second prong of the Wikimedia Allegation centers on showing that the NSA is monitoring at least one of these chokepoint cables.

The problem for Wikimedia is that the NSA never uses the words "chokepoint cable" in its public disclosures. The NSA does, however, use the phrase "international Internet link." The parties therefore dispute whether those terms are interchangeable, and even if they are, whether the relevant disclosures reveal that the NSA is actually monitoring such a circuit.

At the outset, we focus on the government's concession in the 2011 FISC opinion and not the Coats declaration (on which the district court relied). As Wikimedia acknowledges, Director Coats's statement that the NSA is "monitoring at least one circuit carrying international Internet communications," J.A. 186, doesn't identify where on the

Internet backbone that circuit is located. The Coats declaration thus doesn't show that the NSA is monitoring a chokepoint cable.

By contrast, the FISC opinion recites a government concession in that case "that [the] NSA will acquire a wholly domestic 'about' communication if the transaction containing the communication is routed through *an international Internet link being monitored by [the] NSA*." *Redacted*, 2011 WL 10945618, at *15 (emphasis added). According to Wikimedia, this concession—the accuracy of which the NSA has confirmed in this case—is evidence that NSA is in fact monitoring a circuit carrying international communications.

The government argues that the statement from the FISC opinion doesn't reveal that the NSA is actually monitoring an international Internet link. Rather, it conveys only that *if* the NSA is monitoring such a link, the agency will acquire the communications traversing it. But the government's strained construction ignores grammar. The consequence described in the independent clause (i.e., the NSA's acquisition of a domestic communication) is tied to a conditional clause that turns on whether the transaction is on an international Internet link that the NSA is monitoring—not whether the NSA is monitoring such a link at all. The sentence is thus premised on the NSA surveilling at least one international Internet link, over which a transaction of interest may travel.

The government also says that Wikimedia has no evidence that the NSA still adheres to these practices, even if it did in 2011, and that "at least the conclusion of this conditional statement is no longer accurate" because "'about' collection ended in 2017." Appellee's Br. at 40 n.3 (quoting *Wikimedia Found.*, 427 F. Supp. 3d at 602 n.38). But the government

never says that the way it acquired "about" communications differs from the way it collects "to" and "from" communications. Nor have we seen anything in the record to suggest that.

To the contrary, Upstream collection is often described as a single process across all types of communications. *See, e.g., Redacted*, 2011 WL 10945618, at *11 ("[The] NSA's upstream Internet collection devices are 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."). And given the lack of evidence that the NSA has changed the way it operates Upstream, it's reasonable to infer that the government's concession in the FISC opinion remains accurate despite the passage of time and even though the government no longer retains "about" communications.

Next, the government argues that Wikimedia didn't dispute the district court's determination that "the differences between the term 'international internet link' and the term ['chokepoint cable'] . . . cannot be known without violation of the state secrets privilege." *Wikimedia Found.*, 427 F. Supp. 3d at 602. Because the "opening brief does not mention the district court's ruling on this point, much less argue that the court erred or explain how [it erred]," the government contends that Wikimedia failed to preserve this issue. Appellee's Br. at 41 (citing *Grayson O Co. v. Agadir Int'l LLC*, 856 F.3d 307, 316 (4th Cir. 2017)).

But it's not clear that the district court actually ruled on the definition of "international Internet link," as opposed to merely describing the government's position on it. *See Wikimedia Found.*, 427 F. Supp. 3d at 602 ("Defendants, however, assert . . . .

Thus, the differences between the term . . . ."). The court then turned away from the FISC opinion to focus on the Coats declaration, suggesting that the court didn't intend to resolve the significance of "international Internet link" at all—on state secrets or any other grounds. *Id.* at 602–03.

Even if the court was commenting on the secret nature of the phrase "international internet link," it ultimately found for Wikimedia on the second prong. Wikimedia thus had no reason to raise any arguments on the second prong before the government contested it.[8] *See Nw. Airlines, Inc. v. Cnty. of Kent*, 510 U.S. 355, 364 (1994) ("A prevailing party need not . . . defend a judgment on any ground properly raised below, so long as that party seeks to preserve, and not to change, the judgment.").

The government argues that the meaning of "international Internet link" is in fact classified and that Wikimedia thus lacks evidence showing that the meaning of those words as used in the FISC opinion is the same as that used in the Wikimedia Allegation. But the government's insistence that the true definition of this phrase is a secret doesn't invalidate its concession in the FISC opinion as "concrete evidence from which a reasonable juror could return a verdict in [Wikimedia's] favor." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 256 (1986). Even if "international Internet link" could conceivably be code for

[8] In any event, Wikimedia's opening brief explains how the FISC opinion supports the second prong based on publicly available information. This preserves its arguments on the point. *See* Appellant's Br. at 25–27; *see also Blackwelder v. Millman*, 522 F.2d 766, 771 (4th Cir. 1975) (holding that a prevailing party "may support the judgment by urging any theory, argument, or contention which is supported by the record, even though it was specifically rejected by the lower court").

anything from a chihuahua to a chandelier, it's sensible to infer that the FISC opinion uses that phrase to refer to a chokepoint cable.[9]

Indeed, the ordinary meaning of "international Internet link" is a connection carrying Internet traffic between two countries. And its usage in describing Upstream surveillance suggests that one of those countries must be the United States. *See, e.g.*, PCLOB Report at 40 ("Upstream collection . . . [occurs] with the compelled assistance (through a Section 702 directive) of the providers that control the telecommunications backbone . . . . The collection therefore *does not occur at . . . foreign telephone or Internet companies*, which the government cannot compel to comply with a Section 702 directive." (emphasis added)); *id.* at 36–37 ("Once tasked, selectors used for the acquisition of upstream Internet transactions are sent to a *United States electronic communication service provider* to acquire communications that are transiting through . . . the 'Internet backbone.'" (emphasis added)); J.A. 1003 (Bradner Decl.) ("This of course makes sense, given that public Internet traffic on [chokepoint cables] . . . is the traffic that the NSA is authorized to monitor under its Section 702 procedures.").

To be sure, "whether an inference is reasonable cannot be decided in a vacuum; it must be considered in light of the competing inferences to the contrary." *Sylvia Dev. Corp.*, 48 F.3d at 818 (cleaned up). But the government doesn't offer any evidence suggesting that "international Internet link" has a counterintuitive meaning. Wikimedia's

[9] Wikimedia also argues that it's reasonable to infer from government disclosures that the NSA is monitoring multiple chokepoints. But this assertion is superfluous to what Wikimedia must prove for standing, so we don't address it further.

argument that the government's concession in the FISC opinion refers to a chokepoint cable thus falls well "within the range of reasonable probability." *Id.* (quoting *Ford Motor Co. v. McDavid,* 259 F.2d 261, 266 (4th Cir. 1958)). And because we must draw all reasonable inferences in Wikimedia's favor, this is sufficient to establish a genuine issue of material fact as to the second prong of the Wikimedia Allegation.

2.

Wikimedia next argues that summary judgment for the government wasn't appropriate as to the third prong of the Wikimedia Allegation: that the NSA copies all communications on a monitored link. In particular, Wikimedia asserts that this prong is supported by (1) "the government's own disclosures"; (2) the "technical and practical necessities" of conducting Upstream surveillance; and (3) the NSA's goal of "comprehensively acquir[ing] communications that are sent to or from its targets." Appellant's Br. at 28–30. Relatedly, Wikimedia contends that the court shouldn't have excluded a portion of Bradner's expert opinion when assessing this prong.

We agree in part. Because reasonable inferences drawn from the government's concession in the FISC opinion establish a genuine issue of material fact as to the third prong, the district court erred in granting summary judgment to the government.

The government doesn't dispute that Wikimedia may prove the third prong by showing that the NSA is copying all transactions on a monitored link by choice, as Wikimedia urges now, rather than by technological necessity, as it argued at the motion-to-dismiss stage. This shift in focus is hardly surprising, given Wikimedia's

acknowledgment that it's technically feasible to conduct Upstream surveillance without copying all communications on a monitored link.

The district court, when discussing the third prong of the Wikimedia Allegation, made no mention of most of the government disclosures Wikimedia cited for its claim that the NSA is copying all communications transiting a monitored link by choice. To the extent that the court touched on copying by choice at all, it did so only in the context of excluding from its analysis Bradner's expert opinion that discusses why the NSA might prefer link-layer copying or optical splitters (which both result in wholesale copying). We thus conduct the analysis that the district court passed on: whether Wikimedia "set forth specific facts showing that there is a genuine issue for trial" with respect to the allegation that the NSA has elected to copy all transactions on a surveilled circuit. *Lujan v. Nat'l Wildlife Fed.*, 497 U.S. 871, 888 (1990).

As support for this proposition, Wikimedia again leads with the same statement from the 2011 FISC opinion, this time highlighting a different portion of it. The government's concession in that case that the "NSA *will acquire* a domestic 'about' communication if the transaction containing the communication is routed through an international Internet link being monitored by [the] NSA" can only be true, says Wikimedia, if the NSA is copying all traffic on a surveilled circuit.[10] *Redacted*, 2011 WL 10945618, at *15 (emphasis added).

[10] The "will acquire" language also appears once more in the FISC opinion, expressing essentially the same notion. *See Redacted*, 2011 WL 10945618, at *11 ("[The] NSA likely acquires tens of thousands more wholly domestic communications every year,

The government says that this portion of the FISC opinion lacks technical precision. In particular, it points to another part of the FISC opinion that says the "NSA *may acquire* wholly domestic communications," *id.* at *11 n.34 (emphasis added), which it claims is inconsistent with the "will acquire" statement. This argument, however, takes the "may acquire" quote out of context.

The "may acquire" phrase comes from a portion of the opinion describing a specific kind of transaction (a multi-communication transaction), and not how transactions on a monitored link are generally acquired. One or more of the discrete communications contained within a single multi-communication transaction may be wholly domestic but the NSA may "lack[] sufficient information . . . to determine the location or identity" of the sender. *Id.* Accordingly, "[the] NSA *may acquire* wholly domestic communications" within a particular multi-communication transaction without knowing that it has done so.[11] *Id.* (emphasis added). But this says nothing about how the NSA obtained the multi-communication transaction—i.e., whether it's because, as Wikimedia alleges, the NSA is copying all transactions on a monitored link.

The government also offers a competing interpretation of its concession in the FISC opinion. It argues that the "will acquire" quote doesn't mean the NSA acquires *every*

---

given that [the] NSA's upstream collection devices *will acquire* a wholly domestic 'about' [communication] if it is routed internationally." (emphasis added)).

[11] In fact, when the NSA manually reviewed a random sample of transactions collected through Upstream, it couldn't "determine conclusively" whether 224 out of 5,081 multi-communication transactions contained wholly domestic communications. *Redacted*, 2011 WL 10945618, at *11 n.34.

domestic communication on a monitored link. Why? Because, posits the government, the relevant sentence says only the NSA will acquire "a" domestic communication, not "all" such communications. While literally true, the government's myopic reading ignores the significance of the word "a" in context.

As an indefinite article, "a" can mean "any" and precedes a "singular noun[] when the referent is unspecified." *A*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/a (last visited August 18, 2021). Therefore, the best reading of the government's concession is that the NSA "will acquire" any single, unspecified domestic communication, so long as it's traversing a monitored international Internet link. In the context of the "will acquire" sentence then, the NSA's surefire acquisition of "a" domestic communication on a surveilled circuit is equivalent to its acquisition of "all" such transactions.

Judge Rushing says that we take the government's concession in the FISC opinion out of context. Not so. The fact that the "will acquire" phrase appears in a section of the FISC opinion explaining that the NSA intentionally designed its collection devices to acquire wholly domestic communications is entirely consistent with the inference that the NSA has chosen to copy all communications on a monitored link.

Moreover, the government's concession isn't a stray statement swimming against a tide of contrary text. In fact, only a few subparts of the eighty-page FISC opinion are relevant to how the NSA acquires transactions. *See Redacted*, 2011 WL 10945618, at *9–16 (discussing the scope of the NSA's Upstream collections and the NSA's targeting procedures). And it's telling that the FISC opinion recites the "will acquire" language a

second time, *see id.* at *11, when describing the government's collection of wholly domestic communications in a portion of the opinion dedicated to "the comprehensiveness of the NSA's collection practices," Dissent at 66. Indeed, neither the government nor my colleague have pointed to a single sentence in the other seventy-nine pages of the FISC opinion that refutes Wikimedia's interpretation of the government's concession.[12]

3.

Wikimedia's "grab-bag" of other support for the third prong, Appellee's Br. at 51, doesn't contain standalone proof that the NSA is copying before filtering. For example, the NSA's desire to be "comprehensive[]" in its surveillance, PCLOB Report at 10, 123, doesn't necessarily mean that its collection of communications is exhaustive, especially given the agency's technical, logistical, and financial restraints in the face of competing mission priorities—all of which are classified.

But Wikimedia's supplemental evidence is at least consistent with its reasonable interpretation of the government's concession in the FISC opinion, and the government again fails to offer any contradictory evidence that casts doubt on those inferences.

[12] At best, Judge Rushing's belief that the government's concession in the FISC opinion can be reasonably interpreted another way confirms that Wikimedia has raised a genuine issue of material fact sufficient to preclude summary judgment. *See W. C. English, Inc. v. Rummel, Klepper & Kahl, LLP*, 934 F.3d 398, 404 (4th Cir. 2019) (explaining that when there are "two reasonable interpretations" of a phrase, "the granting of summary judgment for either side [is] improper" (cleaned up)).

Wikimedia thus has established a genuine issue of material fact with respect to the third prong of the Wikimedia Allegation and its Article III standing.[13]

B.

Having confirmed our jurisdiction, we now turn to Wikimedia's contention that the court erred in relying on the state secrets privilege to deny its motion to compel discovery and grant the government's motion to dismiss because § 1806(f) of FISA displaces the privilege.[14] We review de novo both questions of statutory interpretation, *United States v. Abugala*, 336 F.3d 277, 278 (4th Cir. 2003), and "legal determinations involving state secrets," *El-Masri v. United States*, 479 F.3d 296, 302 (4th Cir. 2007). Because we conclude that § 1806(f) is relevant only when a litigant challenges the admissibility of the government's surveillance evidence, it doesn't apply here. Instead, we apply the state secrets privilege and hold, like the district court, that it forecloses further litigation.

---

[13] Because we hold that the case must nonetheless be dismissed because of the state secrets privilege, we don't tackle Wikimedia's claim that the district court abused its discretion in excluding some of Bradner's opinions. Nor do we address Wikimedia's arguments about the merits of Schulzrinne's opinions.

[14] Judge Motz chides us for (as she describes it) rushing to decide this issue in the face of the Supreme Court's grant of certiorari in *Fazaga*. But this case was briefed and argued months before the Court decided to take *Fazaga*, and we have given it all due deliberation. Moreover, our superior Court is often informed by the views of the circuits. *See, e.g., Hertz Corp. v. Friend*, 559 U.S. 77, 92 ("In an effort to find a single, more uniform interpretation of the statutory phrase, we have reviewed the Courts of Appeals' divergent . . . interpretations."). As we've done in the past, we respectfully offer our perspective on this "novel and difficult question" (Dissent at 56) before the Court provides a definitive answer. *See, e.g., Int'l Refugee Assistance Project v. Trump*, 883 F.3d 233 (4th Cir. 2018) (affirming the district court's grant of a preliminary injunction despite the Supreme Court's grant of a writ of certiorari on the same issues).

1.

The parties first debate the origin of the state secrets privilege. Wikimedia calls it a common law privilege, which Congress can abrogate by passing a statute that "speak[s] directly to the question addressed by" the privilege, even if the statute doesn't "affirmatively proscribe it." *United States v. Texas*, 507 U.S. 529, 534 (1993). The government says the privilege is "constitutionally grounded," Appellee's Br. at 11, and can only be supplanted where "Congress specifically has provided" for a statute to do so. *Dep't of Navy v. Egan*, 484 U.S. 518, 530 (1988).

We have indeed observed that the state secrets privilege is an evidentiary rule "bas[ed] in the common law of evidence." *El-Masri*, 479 F.3d at 303–04; *see also Gen. Dynamics Corp. v. United States*, 563 U.S. 478, 485 (2011) ("*Reynolds* . . . decided a purely evidentiary dispute by applying evidentiary rules."). But we've also recognized that the privilege "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; *see also United States v. Nixon*, 418 U.S. 683, 711 (1974) ("[T]o the extent [an evidentiary privilege] relates to the effective discharge of a President's powers, it is constitutionally based.").

Fortunately, we need not decide today who has the better argument. As we explain, even if we agree with Wikimedia that the state secrets privilege is grounded in the common law (which Congress may abrogate), FISA doesn't "speak directly" to the situation here. *Texas*, 507 U.S. at 534.

2.

a.

"We begin, as always in deciding questions of statutory interpretation, with the text of the statute." *Othi v. Holder*, 734 F.3d 259, 265 (4th Cir. 2013). The relevant subsection of FISA provides:

> Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, 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.

50 U.S.C. § 1806(f). FISA further defines an "aggrieved 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." *Id.* at § 1801(k).

The first lines of this subsection describe three conditions that trigger the district court's in camera and ex parte review obligations. These are: (i) when the federal or state government notifies the court that it intends to use electronic surveillance information

against an aggrieved person, which it's required to do before introducing such evidence in a judicial proceeding under § 1806(c) or (d); (ii) when an aggrieved person makes a motion to suppress electronic surveillance information used by the government under § 1806(e); and (iii) when an aggrieved person makes "any motion or request . . . pursuant to any other statute or rule . . . 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." *Id.* at § 1806(f).

b.

Relying heavily on *Fazaga*, Wikimedia claims that the third condition unambiguously encompasses the circumstances at hand: Wikimedia is an aggrieved person that made a motion before the district court under Federal Rule of Civil Procedure 37(a) to compel discovery of "materials relating to electronic surveillance." *Id.* at § 1806(f). Wikimedia thus reads § 1806(f) as a free-floating right to obtain information related to the government's electronic surveillance pursuant to any (and all) federal statutes or rules.

But "[t]he plainness or ambiguity of statutory language is determined by reference to the language itself, the specific context in which that language is used, and the broader context of the statute as a whole." *Healthkeepers, Inc. v. Richmond Ambulance Auth.*, 642 F.3d 466, 471 (4th Cir. 2011) (quoting *Robinson v. Shell Oil Co.*, 519 U.S. 337, 340 (1997)). "This includes employing various grammatical and structural canons of statutory interpretation which are helpful in guiding our reading of the text." *Id.* (citing *United Sav. Ass'n. v. Timbers of Inwood Forest Assocs.*, 484 U.S. 365, 371 (1988)).

Reading the third condition in context reveals that Wikimedia's gloss makes for a shiny but ill-fitting shoe. Both parties agree that § 1806(f) may apply regardless of who initiated the suit. But we agree with the government that § 1806(f) describes procedures for determining the admissibility of electronic surveillance information only when the *government* seeks to use such evidence in a particular proceeding—whether civil or criminal. Thus, even assuming that Wikimedia is an aggrieved person,[15] we conclude that it can't use § 1806(f) to force the government to introduce electronic surveillance information into this case. To the extent our reasoning, as laid out below, is inconsistent with *Fazaga*, we decline to follow our sister circuit.

"[W]e rely on the principle of *noscitur a sociis*—a word is known by the company it keeps—to avoid ascribing to one word a meaning so broad that it is inconsistent with its accompanying words, thus giving unintended breadth to the Acts of Congress." *Yates v. United States*, 574 U.S. 528, 543 (2015) (cleaned up). Both of the specific conditions in § 1806(f) (notice of government intent to use surveillance information and a motion to suppress) presume the government's introduction of surveillance evidence into the proceedings. The subsequent general condition "is therefore appropriately read to refer, not to any [motion]," as Wikimedia asserts, "but specifically to the subset" of motions contingent on the government's use of surveillance evidence. *Id.* at 544; *see also id.* at 543

[15] Given our assumption, we don't have to determine what a litigant must prove to qualify as an aggrieved person and whether Wikimedia has done so.

(explaining that the meaning of a word in a list may be limited by the other enumerated terms, "even though the list began with the word 'any'").

Relatedly, where "general words follow specific words in a statutory enumeration," the *ejusdem generis* canon counsels that "the general words are construed to embrace only objects similar in nature to those objects enumerated by the preceding specific words." *Wash. State Dep't of Soc. & Health Servs. v. Guardianship Estate of Keffeler*, 537 U.S. 371, 384 (2003); *see also CSX Transp., Inc. v. Ala. Dept. of Revenue*, 562 U.S. 277, 295 (2011) ("We typically use *ejusdem generis* to ensure that a general word will not render specific words meaningless."). Here, if § 1806(f)'s third condition requiring the district court to act on "any motion or request" were as "all encompassing" as Wikimedia alleges, it would render the second condition superfluous. *See Yates*, 574 U.S. at 546. "Congress would have had no reason to refer specifically to [motions to suppress]"—in fact, it's "hard to see why [Congress] would have needed to include the examples at all." *Id.* at 545–46.

It makes more sense to conclude that, by including the two preceding conditions, Congress signaled its intent to "cabin the contextual meaning" of the third condition. *Id.* at 543. Like its predecessors, the third condition thus applies only when an aggrieved person makes a motion or request *in response* to the government's attempt to use surveillance evidence in a proceeding.

This interpretation accords with the limitations that Congress attached to the third condition on the back end. Section 1806(f) specifies that the litigant's motion must be "to discover, obtain, or suppress." These are familiar "procedural motions pertaining to the admissibility of evidence." *Fazaga*, 965 F.3d at 1083 (Butamay, J. dissenting). The direct

objects of those actions are the "applications or orders or other materials relating to electronic surveillance" or the "evidence or information obtained or derived from [such] surveillance." 50 U.S.C. § 1806(f). And the district court's review is correspondingly restricted to the "application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance . . . was lawfully authorized and conducted." *Id.*

Here, too, *noscitur a sociis* and *ejusdem generis* color our understanding of "other material" and "such other material" to mean those like a FISA application or order—i.e., documents related to officially approving and defining the scope of FISA surveillance that can thus be used to determine the legality of the government's surveillance operations. *See also Such*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/such (last visited August 18, 2021) (defining "such" as "of the character, quality, or extent previously indicated or implied").

In short, the third condition in § 1806(f) is confined to procedural requests related to a circumscribed body of evidence (i.e., the government's FISA documentation and the resulting intelligence). This corresponds with interpreting § 1806(f) as directed towards determining the admissibility of the fruits of the government's surveillance—a question that arises only when the government offers such evidence in a case—and not as an unbounded invitation for litigants to acquire any information they desire about the government's intelligence programs.

c.

The remedy available to a successful movant confirms our reading of this condition. As the very next subsection provides:

> 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.

50 U.S.C. § 1806(g).

The paradigmatic remedy is thus the suppression of evidence. It's even the focus of the subsection's title: "Suppression of evidence; denial of motion." *Id.*; *see also Fla. Dept. of Revenue v. Piccadilly Cafeterias, Inc.*, 554 U.S. 33, 47 (2008) ("[A] subchapter heading cannot substitute for the operative text of the statute. Nonetheless, statutory titles and section headings are tools available for the resolution of a doubt about the meaning of a statute." (cleaned up)).[16] And a litigant would seek such a remedy only in response to the government's introduction of surveillance evidence into the case.

By contrast, consider the mismatch between the remedy described in § 1806(g) and the remedy that Wikimedia seeks. Rather than request the suppression of evidence, Wikimedia wants the district court to review the evidence requested by the motion to

[16] The titles of § 1806 as a whole, "Use of information," and § 1806(f), "In camera and ex parte review by district court," are less illuminating but remain consistent with the notion that it's the government's use of information that matters.

compel to decide both standing and the merits of its unlawful surveillance claims. But that approach would contort the §1806(f) and (g) procedures beyond recognition. The statutory text doesn't permit the district court to rule on anything other than the motion at hand or consider evidence beyond the FISA application and related materials, let alone conduct an entire trial in camera and grant final judgment on the merits of the underlying claim.[17]

We note that every other subsection under § 1806 speaks to the government's use of electronic surveillance evidence. Section 1806(a) provides that such evidence "may be used and disclosed by Federal officers and employees" in compliance with minimization procedures; (b) says that such evidence "may only be used in a criminal proceeding with the advance authorization of the Attorney General"; (c) and (d) mandate that federal and state governments give notice before using such information against an aggrieved person; (e) permits an aggrieved person to file a motion to suppress such evidence when used against him; (i) requires that the government destroy information unintentionally acquired through electronic surveillance; (j) instructs a court about notifying an aggrieved person when the government conducts emergency surveillance without pre-authorization; and (k) allows federal officers who conduct electronic surveillance to coordinate with federal or state law enforcement officers.[18] We think it unlikely that Congress stashed away an

[17] Wikimedia argues that this emphasis on motions to suppress is misguided because § 1806(f) expressly includes more than that. Even accepting that as true, we are confident that it doesn't contemplate what Wikimedia seeks in this litigation.

[18] Section 1806(h) is the only subsection that doesn't expressly relate to the government's use of information, but it merely provides that a district court's decisions under subsection (g) are final and binding upon all other federal courts.

expansive right for litigants within a statute directed entirely toward the government's use of information. *See Whitman v. Am. Trucking Ass'ns*, 531 U.S. 457, 468 (2001) ("Congress . . . does not, one might say, hide elephants in mouseholes.").

Still, Wikimedia resists this interpretation, contending that the government's reading effectively means that a plaintiff can only rely on § 1806(f) after the government has given notice that it's using electronic surveillance information per § 1806(c) or (d),[19] which renders the two other conditions for obtaining in camera and ex parte review superfluous. That might be the case if the government were always scrupulous in providing such notice. But even the government admits that there has been some "dispute" about its withholding of notice in the past, though it claims to have "redoubled its efforts" since the Solicitor General's 2013 confession of error on this front. Oral Argument at 35:07–35:56.

It's therefore reasonable for Congress to have crafted additional paths for ascertaining the legality of electronic surveillance evidence that the government intends to marshal against a litigant who can show that it is an "aggrieved person," even when the government has violated its duty to provide notice of such use. *Cf. United States v. Belfield*, 692 F.2d 141, 146 (D.C. Cir. 1982) (explaining that a litigant "claim[ing] that he has been the victim of an illegal surveillance [operation] and seek[ing] discovery of the [surveillance records] to ensure that no fruits thereof are being used against him" can trigger the

[19] As mentioned above, § 1806(c) and (d) require federal and state governments, respectively, to give notice to the court or to the aggrieved person when they intend to use surveillance evidence against such a person in a judicial proceeding.

§ 1806(f) procedures even though the government "has purported not to be offering any [such] evidence").

Additionally, Wikimedia asserts that the phrase "notwithstanding any other law" is an indication that FISA displaces the state secrets privilege. But that clause applies only when the plaintiff has fulfilled one of the three pre-requisite conditions for triggering the court's in camera and ex parte review, and the Attorney General has filed the necessary affidavit. Only then "shall" the court apply the § 1806(f) in camera procedures, "notwithstanding any other law" that would require some other, public resolution of the litigant's motion challenging the government's use of electronic surveillance information. *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. . . . This is necessary to prevent the carefully drawn procedures in subsection [(f)] from being bypassed by the inventive litigant using a new statute, rule or judicial construction.").[20]

And although § 1806(f) and the state secrets privilege are triggered by an affidavit from the government, it doesn't follow that FISA speaks directly to the state secrets privilege, as Wikimedia claims. Tellingly, these procedures contemplate different affiants. Because the privilege is a shield to protect state secrets from disclosure, the head of the

[20] In the draft of the statute discussed by this report, what is now subsection (f) was located under subsection (e). *See* S. Rep. No. 95-701, at 88. Despite the different lettering, the substance of the provision was largely the same. We have edited the quote to correspond with the current organization of § 1806's provisions.

department controlling the information must assert it. By contrast, FISA applies when the government is attempting to offer electronic surveillance evidence in a case. In such an instance, responsibility for invoking § 1806(f) falls to the one who wields the sword: the Attorney General (or his delegees, under 50 U.S.C. § 1801(g)). The triggering mechanisms for each procedure thus strengthen the inference that FISA wasn't intended to displace the state secrets privilege.

d.

Wikimedia further contends that limiting the applicability of § 1806(f) and (g) to when the government offers electronic surveillance evidence in a case is inconsistent with FISA as a whole. In particular, Wikimedia complains that if § 1806(f) doesn't displace the state secrets privilege, the government can invoke the privilege "in *every* FISA suit brought by a civil plaintiff." Reply Br. at 5. This would, in turn, give the government "nearly exclusive control over challenges to FISA surveillance" and "profoundly undermine the civil remedies that Congress enacted for surveillance abuses[] and the very purpose of FISA itself," which Wikimedia asserts is "to ensure judicial review of executive branch surveillance." Appellant's Br. at 51–52.

We are not convinced. The government knows that it carries the burden "to satisfy the reviewing court that the *Reynolds* reasonable-danger standard is met," *Abilt v. CIA*, 848 F.3d 305, 312 (4th Cir. 2017) (cleaned up), and that the judiciary is "firmly in control of deciding whether an executive assertion of the state secrets privilege is valid," *El-Masri*, 479 F.3d at 304–05. Indeed, the court stands as a gatekeeper to the privilege, and "[w]e take very seriously our obligation to review the [government's claims] with a very careful,

indeed a skeptical, eye," *Abilt*, 848 F.3d at 312 (quoting *Al–Haramain Islamic Found., Inc. v. Bush*, 507 F.3d 1190, 1203 (9th Cir. 2007)), so that "the state secrets privilege is asserted no more frequently and sweepingly than necessary," *id.* (quoting *Ellsberg v. Mitchell*, 709 F.2d 51, 58 (D.C. Cir. 1983)). There have thus been FISA cases where the government hasn't invoked the privilege, *see, e.g.*, *Am. Civil Liberties Union v. Clapper*, 785 F.3d 787, 801–03 (2d Cir. 2015), or has invoked the privilege narrowly, *see, e.g.*, *Fazaga*, 965 F.3d at 1042 ("Here, although the Government has claimed the *Reynolds* privilege over certain state secrets, it has not sought dismissal of the Fourth Amendment and FISA claims based on its invocation of the privilege.").

Nor do we see any actual contradictions between FISA and the *Reynolds* privilege. Congress provided for judicial review of executive branch surveillance, but it did so to "strike[] a fair and just balance between protection of national security and protection of personal liberties." S. Rep. No. 95-604, pt. 1, at 7 (1978). The government's reading of § 1806(f) fits that schema exactly. In that provision, Congress permits the government to use electronic surveillance evidence in court against a litigant while withholding materials related to that surveillance from that individual in the interests of national security. But in the same breath, Congress also allows an aggrieved person to challenge the government's use of such evidence and have a court evaluate the lawfulness of the government's actions.

Far from giving the government exclusive control over challenges to surveillance, we think this reading of § 1806(f) acknowledges the court's role in preserving the compromise Congress made between individual rights and national security. *See Belfield*, 692 F.2d at 149 ("If anything, the legality inquiry mandated by FISA is easier for a court

to perform *ex parte* than the pre-FISA inquiry into the legality of warrantless electronic surveillance . . ."). For instance, when "the Court believes that disclosure is necessary to make an accurate determination of legality, but the Government argues that to do so . . . would damage the national security," § 1806(f) says that "the Government must choose—either disclose the material or forgo the use of the surveillance-based evidence." *See* S. Rep. No. 95-701, at 65.

Additionally, judicial review occurs at another point in the FISA process. "Congress created a comprehensive scheme in which the [FISC] evaluates the Government's certifications, targeting procedures, and minimization procedures—including assessing whether the targeting and minimization procedures comport with the Fourth Amendment," *Clapper*, 568 U.S. at 421, which we described more fully in our prior opinion, *see Wikimedia Found.*, 857 F.3d at 200–01. "Any dissatisfaction that [Wikimedia] may have about the [FISC]'s rulings—or the congressional delineation of that court's role—is irrelevant" to our analysis. *Clapper*, 568 U.S. at 421.

In sum, the government's reading of § 1806 is entirely consistent with ensuring judicial review of executive branch surveillance. That's not surprising considering the history of courts uniformly using in camera procedures to determine the legality of foreign-intelligence surveillance even before FISA's enactment. *See Belfield*, 692 F.2d at 149 & n.38 (collecting cases). As the government observes, "[t]hat such [in camera] procedures comfortably coexisted with the [state secrets] privilege before FISA underscores that codification of *in camera* procedures for certain purposes," without more, doesn't suggest that Congress intended to displace the privilege. Appellee's Br. at 35; *see also* H.R. Rep.

No. 95-1283 (1978) ("[O]nce the surveillance is determined to be unlawful, the intent of [§ 1806] is to leave to otherwise existing law the resolution of what, if anything, is to be disclosed.").

The only "inconsistency" between FISA and the state secrets privilege Wikimedia identifies is that Congress provided civil remedies for violations of FISA that a plaintiff may have to forego when the government invokes the *Reynolds* privilege. These include 50 U.S.C. § 1810, whereby a plaintiff may recover damages from a person who is criminally prosecuted under 50 U.S.C. § 1809 for intentionally engaging in, disclosing, or using electronic surveillance in violation of FISA; and 18 U.S.C. § 2712, which permits a plaintiff to recover damages from the United States for a willful violation of FISA.

But this problem isn't unique to FISA. Every state secrets case presents the possibility that a plaintiff will be denied—in the interests of national security—a remedy available by law. *See El-Masri*, 479 F.3d at 313 ("[T]he successful interposition of the state secrets privilege imposes a heavy burden on the party against whom the privilege is asserted . . . not through any fault of his own, but because his personal interest in pursuing his civil claim is subordinated to the collective interest in national security."); *Fitzgerald v. Penthouse Int'l, Ltd.*, 776 F.2d 1236, 1238 n.3 ("When the state secrets privilege is validly asserted, the result is unfairness to individual litigants—through the loss of important evidence or dismissal of a case—in order to protect a greater public value."); *Sterling v. Tenet,* 416 F.3d 338, 348 (4th Cir. 2005) ("[I]n limited circumstances like these, the fundamental principle of access to courts must bow to the fact that a nation without sound intelligence is a nation at risk.").

Accordingly, we conclude that § 1806(f) doesn't displace the state secrets privilege, even in actions pertaining to government-run electronic surveillance.

3.

Because FISA's discovery procedures don't govern here, we turn to whether the district court properly applied the state secrets privilege. We hold that the privilege indeed requires dismissal of this case.

a.

When a state secrets question arises, a court applies a three-part analysis. First, "the court must ascertain that the procedural requirements for invoking the state secrets privilege have been satisfied"—i.e., that the government properly made a formal claim of privilege. *El-Masri*, 479 F.3d at 304. Wikimedia doesn't dispute that the government satisfied this condition.

Second, "the court must decide whether the information sought to be protected qualifies as privileged" because it is a state secret. *Id.* That is, it must determine, "from all the circumstances of the case," whether "there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged." *Reynolds*, 345 U.S. at 10.

This inquiry "pits the judiciary's search for truth against the Executive's duty to maintain the nation's security." *El-Masri*, 479 F.3d at 305. Accordingly, "[t]he degree to which such a reviewing court should probe depends in part on the importance of the assertedly privileged information to the position of the party seeking it": "where there is a strong showing of necessity, the claim of privilege should not be lightly accepted," but

"even the most compelling necessity cannot overcome the claim of privilege if the court is ultimately satisfied that [state] secrets are at stake." *Id.*

b.

The district court found that "the entities subject to Upstream surveillance activity and the operational details of the Upstream collection process" were state secrets because their disclosure "would (i) undermine ongoing intelligence operations, (ii) deprive the NSA of existing intelligence operations, and significantly, (iii) provide foreign adversaries with the tools necessary both to evade U.S. intelligence operations and to conduct their own operations against the United States and its allies." *Wikimedia Found.*, 427 F. Supp. 3d at 613. The court thus sustained the government's claim of privilege for the seven categories of information identified by the NSA.

Wikimedia doesn't meaningfully dispute the court's finding on this prong either. Instead, it quibbles that to the extent the seven categories cover material that the government has already disclosed, the district court's ruling is overly broad. But we don't read the court's decision to make privileged what's already public. The court instead concluded that because of the state secrets privilege, Wikimedia couldn't compel the government to produce, or otherwise continue to pursue litigation that would risk the disclosure of, additional information related to those categories. *See Wikimedia Found.*, 427 F. Supp. 3d at 611.

And based on the totality of the circumstances, including the Coats and Barnes affidavits, we agree that "there is a reasonable danger" to national security should these facts be disclosed. *El-Masri*, 479 F.3d at 305; *see also id.* ("Frequently, the explanation of

the department head who has lodged the formal privilege claim . . . is sufficient to carry the Executive's burden.").

This leads us to the third step, which is to resolve "how the matter should proceed in light of the successful privilege claim." *El-Masri*, 479 F.3d at 304. Once a court determines that certain facts are state secrets, they are "absolutely protected from disclosure." *Id.* at 306. "[N]o attempt is made to balance the need for secrecy of the privileged information against a party's need for the information's disclosure." *Id.*

As a result, "[i]f a proceeding involving state secrets can be fairly litigated without resort to the privileged information, it may continue." *Id.* But if "any attempt to proceed will threaten disclosure of the privileged matters, dismissal is the proper remedy." *Id.* (cleaned up). The latter situations include where: (1) "the plaintiff cannot prove the prima facie elements of his or her claim without privileged evidence"; (2) "even if the plaintiff can prove a prima facie case without resort to privileged information, . . . the defendants could not properly defend themselves without using privileged evidence"; and (3) "further litigation would present an unjustifiable risk of disclosure." *Abilt*, 848 F.3d at 313–14.[21]

[21] Wikimedia asserts (without further explanation) that the third basis for invoking the state secrets privilege "wrongly collapses the *Reynolds* privilege and the *Totten* [*v. United States*, 92 U.S. 105 (1876)] bar." Appellant's Br. at 58 n.19 (citing *Gen. Dynamics*, 563 U.S. at 485). "*Totten* has come to primarily represent . . . a categorical bar on actions to enforce secret contracts for espionage" that leads to dismissal at the pleading stage "without ever reaching the question of evidence," but it rested "on the proposition that a cause cannot be maintained if its trial would inevitably lead to the disclosure of privileged information." *El-Masri*, 479 F.3d at 306 (citing *Totten*, 92 U.S. at 107; *Reynolds* 345 U.S. at 11 n.26). *Abilt* held that dismissal is appropriate in such a circumstance, and we are bound by circuit precedent.

Here, the district court determined that both the second and third situations apply such that "dismissal is the appropriate, and only available, course of action." *Wikimedia Found.*, 427 F. Supp. 3d at 611. Wikimedia now argues that because it established a prima facie case for standing using public evidence, the court should have reviewed the purportedly privileged material in camera to determine the validity—or at least the existence—of the government's hypothetical defense before ordering the case dismissed.

We agree with the district court that in camera review in this instance would fly in the face of the state secrets privilege as espoused by "both Supreme Court precedent and our own cases." *Sterling*, 416 F.3d at 345. A district court may consider any evidence it deems necessary at step two of the *Reynolds* inquiry—i.e., when determining whether the information at issue comprises state secrets. *See id.* ("There may . . . be cases where the necessity for evidence is sufficiently strong and the danger to national security sufficiently unclear that in camera review of all materials is required to evaluate the claim of privilege."). But after a court makes that determination, the privileged evidence is excised from the case, and not even the court may look at such material in camera. *See id.* ("[W]hen a judge has satisfied himself that the dangers asserted by the government are substantial and real, he need not—indeed, should not—probe further."); *El-Masri*, 479 F.3d at 306 ("On this point, *Reynolds* could not be more specific: 'When the occasion for the privilege is appropriate, the 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.'" (cleaned up)).

Nevertheless, Wikimedia contends that we should hold that a court dismissing a claim in the second situation (for defenses made unavailable by the state secrets privilege) must first determine that the putative defense is "valid," even if that requires limited review of privileged material by the court. *See In re Sealed Case*, 494 F.3d 139, 149 (D.C. Cir. 2007). But even if we adopted that rule—a decision we leave for another day—it wouldn't apply here. In the very case that Wikimedia cites for this proposition, the D.C. Circuit distinguishes between a situation where the government alleges that there are "possible defenses that [the defendant] cannot pursue without resort to privileged materials," in which dismissal is not required unless the government demonstrates that one of those defenses is valid, and where "*any* valid defense . . . would require resort to privileged materials," in which dismissal is warranted without further ado. *Id.* at 149 (emphasis added).

The latter ties into the third condition for dismissal under the state secrets privilege: where "further litigation would present an unjustifiable risk of disclosure." *Abilt*, 848 F.3d at 314. Circumstances in which any valid defense would require resort to privileged materials are those in which "state secrets are so central to [the] proceeding that it cannot be litigated without threatening their disclosure." *El-Masri*, 479 F.3d at 308; *see also In re Sealed Case*, 494 F.3d at 149.

That's the situation here. Wikimedia claims that the NSA is acquiring all communications on a chokepoint cable that it is monitoring. There's simply no conceivable defense to this assertion that wouldn't also reveal the very information that the government is trying to protect: how Upstream surveillance works and where it's

conducted. Indeed, "the whole object of [Wikimedia's] suit and of the discovery" is to inquire into "the methods and operations of the [NSA]"—"a fact that is a state secret."[22] *Sterling*, 416 F.3d at 348.

Wikimedia contends that "the district court need not conclusively determine that Wikimedia is or was in fact subject to Upstream surveillance." Appellant's Br. at 61–62. Even at trial, says Wikimedia, the factfinder need only find by a preponderance of the evidence that the NSA copied Wikimedia's communications.

We, however, can't condone holding a one-sided trial. At the summary-judgment stage, the nonmovant need only support its claims with specific facts that "will be taken to be true." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992). But "at the final stage, those facts (if controverted) must be supported adequately by the evidence adduced at trial." *Id.* (cleaned up). And given that the government's hands are so clearly tied by state secrets, "it would be a mockery of justice for the court" to permit Wikimedia to substantiate its claims by presenting its half of the evidence to the factfinder as if it were the whole. *In re Sealed Case*, 494 F.3d at 148 (quoting *Molerio v. FBI*, 749 F.2d 815, 825 (D.C. Cir. 1984)).

[22] Judge Motz says that the district court could ascertain in camera the validity of the government's "discrete" defenses that (1) it's not copying all communications on a monitored link, and (2) it's hypothetically possible for Upstream to avoid Wikimedia's communications. Dissent at 60-61. Respectfully, a hypothetical is not a defense to reasonable inferences drawn from specific facts (here, a 2011 FISC opinion). Yet that's all the government can offer because how the NSA is actually conducting Upstream is a state secret. That's exactly why the case must be dismissed. In short, there isn't a state secrets problem because the government offers only hypothetical defenses; the government only offers hypothetical defenses because there's a state secrets problem.

The district court thus correctly held that, in the face of the state secrets privilege, Wikimedia can't continue to litigate the Wikimedia Allegation to support standing.[23]

C.

In a last-ditch attempt to avoid dismissal, Wikimedia maintains that Upstream inflicted three additional injuries that independently establish standing without implicating state secrets (and therefore may continue to be litigated): (1) a drop in the readership of certain Wikipedia pages; (2) the cost of implementing protective measures against surveillance over its communications; and (3) third party standing.

On the first, we conclude for substantially the reasons given by the district court that Wikimedia's decline in readership isn't "fairly traceable to the challenged action" such that it confers standing. *Clapper*, 568 U.S. at 409.

The second and third theories of standing aren't actually independent of the Wikimedia Allegation. Both require that Wikimedia establish an injury-in-fact. *See id.* at 402 ("[R]espondents cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending."); *Freilich*, 313 F.3d at 215 ("Our [third-party] standing inquiry involves both constitutional limitations on federal-court jurisdiction and prudential limitations on its exercise. . . . [A] plaintiff must demonstrate . . . an injury-in-fact."). Because further litigation premised on the Wikimedia

[23] Although this case can't proceed to the merits because of the state secrets privilege, that result is not a fait accompli in every case, as Judge Motz fears. Rather, "[t]he effect of a successful interposition of the state secrets privilege by the United States will vary from case to case." *El-Masri*, 479 F.3d at 306.

Allegation—the only remaining and viable injury-in-fact—is foreclosed by the state secrets privilege, so too are these supplementary theories of standing.

* * *

To sum up, evidence of the Wikimedia Allegation establishes a genuine issue of material fact as to standing, but the state secrets privilege prevents further litigation of that issue. And because Wikimedia's other alleged injuries don't support standing, the district court's judgment dismissing this case is

AFFIRMED.

DIANA GRIBBON MOTZ, concurring in part and dissenting in part:

I concur in Parts I and II.A of Judge Diaz's majority opinion. Specifically, I concur in the holding that the district court erred in granting summary judgment as to Wikimedia's standing. But I cannot join the remainder of Judge Diaz's opinion. For reasons unclear to me, both of my colleagues rush to decide a novel and difficult question that the Supreme Court will resolve within the year.

I.

My colleagues conclude that § 106(f) of the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1806(f), does not displace the common law state secrets privilege. *See* Maj. Op. Part II.B.2; Judge Rushing Concurring Op. at 64. Two months ago, the Supreme Court granted certiorari on this very question. *See Fazaga v. Fed. Bureau of Investigation*, 965 F.3d 1015 (9th Cir. 2020), *cert. granted*, 2021 WL 2301971 (U.S. June 7, 2021). I would stay this case pending the outcome of the case before the Supreme Court.

In *Fazaga*, the Ninth Circuit closely examined FISA's text and history and concluded that "the procedures outlined in § 1806(f) [of FISA] . . . constitute Congress's specific and detailed description for how courts should handle claims by the government that the disclosure of material relating to or derived from electronic surveillance would harm national security." *Id.* at 1048 (cleaned up). The *Fazaga* court reasoned that FISA's "plain language, statutory structure, and legislative history demonstrate that Congress

intended FISA to displace the state secrets privilege and its dismissal remedy with respect to electronic surveillance." *Id.* at 1052.

When, as here, the Supreme Court will, in a matter of months, address a question that is central to a case before a lower court, that court should exercise its "inherent" "power to stay proceedings." *Landis v. N. Am. Co.*, 299 U.S. 248, 254 (1936). We have followed precisely this practice in the past, *see Hickey v. Baxter*, 833 F.2d 1005 (4th Cir. 1987) (unpublished table decision) (holding that it was proper to "stay[] proceedings while awaiting guidance from the Supreme Court in a case that could decide relevant issues"), as have our sister circuits, *see, e.g.*, *Chowdhury v. Worldtel Bangladesh Holding, Ltd.*, 746 F.3d 42, 47–48 (2d Cir. 2014); *Golinski v. U.S. Office of Personnel Mgmt.*, 724 F.3d 1048, 1050 (9th Cir. 2013); *Trump Plaza Assocs. v. NLRB*, 679 F.3d 822, 826 (D.C. Cir. 2012). In such cases, staying our hand to await the Supreme Court's guidance "is an expression of prudence, judicial restraint, and respect for the role of a [lower court] that must scrupulously adhere to the instructions of" a higher authority. *Benisek v. Lamone*, 266 F. Supp. 3d 799, 808 (D. Md. 2017). With these principles in mind, I would not attempt to resolve a question that the Supreme Court will soon answer.

II.

Because I would not, at this time, reach the question whether FISA displaces the state secrets privilege, judicial restraint similarly counsels against determining whether the state secrets privilege requires dismissal of Wikimedia's case. I will not do that here. But

I must note that Judge Diaz's state secrets analysis, *see* Maj. Op. Part II.B.3, does raise some serious concerns.[1]

That opinion stands for a sweeping proposition: A suit may be dismissed under the state secrets doctrine, after minimal judicial review, even when the Government premises its only defenses on far-fetched hypotheticals. Maj. Op. at 52. This conclusion marks a dramatic departure from *United States v. Reynolds*, 345 U.S. 1 (1953), and its progeny. And it relegates the judiciary to the role of bit player in cases where weighty constitutional interests ordinarily require us to cast a more "skeptical eye." *Abilt v. CIA*, 848 F.3d 305, 312 (4th Cir. 2017) (cleaned up).

In *Reynolds*, the Supreme Court cautioned that, even in cases implicating national security, "[j]udicial control over the evidence in a case cannot be abdicated to the caprice of executive officers." 345 U.S. at 9–10. Thus, the Court developed a "formula of compromise," mindful that "[t]oo much judicial inquiry into [a] claim of privilege would force disclosure of the thing the privilege was meant to protect, while a complete abandonment of judicial control would lead to intolerable abuses." *Id.* at 8–9.

Under the *Reynolds* framework, before a court passes on a claim of privilege, it must first "determine how far [it] should probe in satisfying itself that the occasion for invoking

[1] Judge Rushing believes that Wikimedia did not demonstrate a dispute of material fact as to its standing, and so she would hold that the Government's motion for summary judgment — not the state secrets doctrine — requires dismissal of this case. *See* Judge Rushing Concurring Op. at 64 (joining only Parts I, II.B.2, and II.C of Judge Diaz's opinion). However, Judge Rushing does agree with Judge Diaz that the Government "successful[ly] assert[ed] [] the state secrets privilege" when opposing Wikimedia's discovery requests. *Id.* at 68.

the privilege is appropriate." *Id.* at 11. This threshold inquiry necessitates considering both the Government's "showing of privilege" and the plaintiff's "showing of necessity." *Id*. On one end of the spectrum, "[w]here there is a strong showing of necessity" or the security threat posed by disclosure is unclear, "the claim of privilege should not be lightly accepted." *Id.*; *Sterling v. Tenet*, 416 F.3d 338, 345 (4th Cir. 2005), *cert. denied*, 546 U.S. 1093 (2006). At the other end, "where necessity is dubious, a formal claim of privilege . . . will have to prevail." *Reynolds*, 345 U.S. at 11.

Applying this framework, the Court in *Reynolds* determined that the plaintiff's "necessity was greatly minimized" by the availability of non-privileged evidence and so a formal claim of privilege — filed by the Secretary of the Air Force — constituted "a sufficient showing of privilege to cut off further demand for the [privileged evidence]." *Id.* at 10–11. The Court concluded that in the case before it, "examination of the [privileged] evidence, even by the judge alone, in chambers" was inappropriate, because a "court should not jeopardize the security which the [state secrets] privilege is meant to protect" when it is confident the privilege applies. *Id.* at 10.

While the *Reynolds* Court refused to "automatically require a complete disclosure to the judge before [a] claim of privilege will be accepted," it expressly recognized that in camera review might sometimes be necessary to evaluate a privilege claim. *Id.*; *Sterling*, 416 F.3d at 345 ("There may of course be cases where the necessity for evidence is sufficiently strong and the danger to national security sufficiently unclear that in camera review of all materials is required to evaluate the claim of privilege."); *see also Doe v. CIA*, 576 F.3d 95, 105 (2d Cir. 2009).

In the decades since *Reynolds*, courts have repeatedly concluded that in camera review is a "necessary process" when, as here, the Government asserts that the state secrets privilege will preclude it from raising a valid defense to a constitutional claim. *Molerio v. FBI*, 749 F.2d 815, 825 (D.C. Cir. 1984) (Scalia, J.); *Fazaga*, 965 F.3d at 1067; *In re Sealed Case*, 494 F.3d 139, 149–51 (D.C. Cir. 2007); *see also Tenenbaum v. Simonini*, 372 F.3d 776, 777 (6th Cir. 2004). Indeed, "allowing the mere prospect of a privileged defense to thwart a citizen's efforts to vindicate his or her constitutional rights would run afoul of the Supreme Court's caution against precluding review of constitutional claims." *In re Sealed Case*, 494 F.3d at 151 (citing *Webster v. Doe*, 486 U.S. 592, 603–04 (1988)). Thus, particularly when constitutional rights are at stake, courts routinely probe a claim of privilege through an "appropriately tailored in camera review" to determine whether "resort to privileged material" is in fact necessary for the Government to pursue a "meritorious and not merely plausible" defense. *Id.* at 149–51.

Judge Diaz eschews this widely adopted approach. Instead, he concludes that we need not scrutinize the Government's claim of privilege because the Government has demonstrated that "*any* valid defense" to Wikimedia's arguments "would require resort to privileged materials." Maj. Op. at 52. My colleague concludes that "state secrets are so central to [the] proceeding that it cannot be litigated without threatening their disclosure," and so the case must be dismissed. *Id.* (quoting *El-Masri v. United States*, 479 F.3d 296, 308 (4th Cir. 2007)).

That simply is not so. The Government has offered two discrete defenses to Wikimedia's standing: (1) that the Government might not engage in Upstream surveillance

at any chokepoint cables carrying Internet traffic between the United States and other countries; and (2) that it is hypothetically possible for Upstream to operate such that the Government filters communications before copying or reviewing them, thus avoiding Wikimedia's communications entirely. Gov't Br. at 39, 44–45, 60. Judge Diaz himself explains at some length that the first defense cannot be reconciled with numerous public disclosures — and simple common sense. Maj. Op. at 22–27. As to the second defense, the Government offers *no* reason why an "appropriately tailored in camera review" could not ascertain the validity of the defense without imperiling state secrets. *In re Sealed Case*, 494 F.3d at 151. As Wikimedia concedes, such review need not probe "the identities of [the Government's] targets, the specific geographic locations where Upstream surveillance is conducted, or the participating companies." Reply Br. at 15–16.

Moreover, the Government's public disclosures and publicly available information about the Internet's workings raise serious doubts about whether privileged material even exists to bolster the Government's second defense. *See* Brief of Amici Curiae Network Engineers and Technologists in Support of Plaintiff-Appellant Wikimedia and Reversal at 3, 12, *Wikimedia Found. v. Nat'l Sec. Agency* (No. 20-1191) (concluding, based on public disclosures and expertise in Internet networking, that the Government's defense "lacks a basis in both Internet technology and engineering" and so "[i]t is highly unlikely, if not virtually impossible," that Upstream's operation resembles the Government's hypothetical).

Judge Diaz suggests that, because the Government offered only totally inadequate hypotheticals as defenses, we must assume — based on nothing more than boilerplate

claims of privilege — that any valid defense would resort to privileged materials. But this turns *Reynolds* on its ear. When the Government makes an inadequate showing, that is precisely when we should not "lightly accept[]" its claims. *Reynolds*, 345 U.S. at 11; *Ellsberg v. Mitchell*, 709 F.2d 51, 59 (D.C. Cir. 1983) (holding that the scope of a court's review should depend on whether the Government's claims are "plausible and substantial"), *cert. denied*, 465 U.S. 1038 (1984); *see also In re United States*, 872 F.2d 472, 479 (D.C. Cir.) (rejecting a claim of privilege after in camera review, notwithstanding the Government's submission of an "affidavit ostensibly describ[ing] the harms that would be dealt to our nation's security . . . were [the] case to continue through the normal course of litigation"), *cert. denied sub nom.*, *United States v. Albertson*, 493 U.S. 960 (1989).

At bottom, my colleague concludes that whenever the Government has not disclosed whether a plaintiff's communications have been subject to FISA surveillance, vague claims of privilege and far-fetched hypotheticals will suffice to obtain dismissal. But FISA surveillance is not a subject that categorically falls outside the bounds of judicial review. *Cf. Tenet v. Doe*, 544 U.S. 1, 9 (2005) (noting that "where the very subject matter of [an] action," such as "a contract to perform espionage, [is] a matter of state secret," a case may be "dismissed on the pleadings without ever reaching the question of evidence, since it [is] so obvious that the action should never prevail over the privilege") (quoting *Reynolds*'s discussion of *Totten v. United States*, 92 U.S. 105 (1876)) (emphasis omitted). And if the *Reynolds* privilege is stretched to require dismissal — before a court may scrutinize the

Government's claims — in cases like this one, I am left to wonder whether *any* electronic surveillance case could *ever* proceed to the merits.[2]

* * *

I recognize that when it considers the issues raised in *Fazaga* and the case at hand, the Supreme Court may bless the majority's approach. But the Court may conclude that the Ninth Circuit properly reconciled "transparency, accountability and national security" in resolving the difficult questions before it. *Fazaga*, 965 F.3d at 1068. The Court may even articulate new factors for lower courts to consider in electronic surveillance cases. In any event, I would await guidance from the Supreme Court.

[2] My colleagues suggest that we should be comforted by the fact that the Government has, in two cases involving FISA surveillance, either declined to invoke the state secrets privilege or declined to seek outright dismissal of some claims pursuant to the privilege. Maj. Op. at 44-45; Judge Rushing Concurring Op. at 64 (joining Part II.B.2 of Judge Diaz's opinion). Recent history indicates that these two cases are outliers. *See* Daniel R. Cassman, Note, *Keep It Secret, Keep It Safe: An Empirical Analysis of the State Secrets Doctrine*, 67 Stan. L. Rev. 1173, 1190–91 (2015) (documenting a dramatic increase in Government assertions of the state secrets privilege, including in FISA cases). In any event, *Reynolds*'s admonition remains applicable: "Judicial control over the evidence in a case cannot be abdicated to the caprice of executive officers." 345 U.S. at 9–10.

RUSHING, Circuit Judge, concurring in part and in the judgment:

I agree with Judge Diaz that FISA's discovery procedures do not govern here, therefore the district court did not err in denying Wikimedia's motion to compel discovery. *See* Maj. Op. Part II.B.2. And I join my colleagues in concluding that Wikimedia's supplementary theories of standing fail. *See* Maj. Op. Part II.C. I write separately because I would also hold that Wikimedia has failed to demonstrate a dispute of material fact regarding its standing based on the Wikimedia Allegation and therefore would affirm the district court's grant of summary judgment on standing grounds.

Summary judgment is proper if Wikimedia—which bears the burden to prove its standing at trial—failed to make a showing sufficient to establish that it has suffered an injury in fact. *See Celotex Corp. v. Catrett*, 477 U.S. 317, 327 (1986); *see also Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). At the summary judgment stage, Wikimedia "can no longer rest on mere allegations but must set forth . . . specific facts" that create a genuine dispute at each necessary step of its standing theory. *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 411–412 (2013) (original alterations and internal quotation marks omitted). The third prong of the Wikimedia Allegation requires Wikimedia to prove that the NSA actually copies and reviews "all the international text-based communications that travel across a given link upon which it has installed surveillance equipment." *Wikimedia Found. v. Nat'l Sec. Agency*, 857 F.3d 193, 210 (4th Cir. 2017) (internal quotation marks omitted). Because much of the information about how the NSA collects communications is shielded from discovery by the state secrets privilege, Wikimedia's task is a difficult one. Unlike the majority, I would hold that Wikimedia has not presented

sufficient evidence from which a reasonable jury could find in its favor on prong three of the Wikimedia Allegation and therefore the Government "is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a); *see also Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 249 (1986) ("[T]here is no issue for trial unless there is sufficient evidence favoring the nonmoving party for a jury to return a verdict for that party.").

The majority hangs its hat on the statement in a declassified 2011 FISC opinion that the "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." *Redacted*, 2011 WL 10945618, at *15 (FISA Ct. Oct. 3, 2011). Wikimedia reads this sentence as conceding that the NSA will acquire *all* wholly domestic "about" communications routed through a monitored link, which, for technological reasons, can only be true if the NSA is copying all traffic on a surveilled circuit. The premise of Wikimedia's argument—that the Government has admitted the NSA collects *all* domestic "about" communications routed through a monitored link—is based not on technological facts, expert opinion, or other evidence in the record but on an unreasonable inference from the 2011 FISC opinion.

By relying on a capacious reading of an indefinite article while ignoring the other eighty pages of the FISC opinion, it is Wikimedia that fails to account for "context." Maj. Op. 31. The section of the 2011 FISC opinion from which Wikimedia plucks its chosen quotation analyzed whether the NSA's acquisition of wholly domestic communications was unintentional. After reviewing the facts concerning collection of both single communication transactions and multiple communication transactions, the FISC concluded

that the collection of wholly domestic communications within those transactions could not be considered unintentional because nothing "suggest[s] that NSA's technical means are malfunctioning or otherwise failing to operate as designed. 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*, 2011 WL 10945618, at *15; *see id.* ("[After] a manual review of a sample of its upstream collection . . . there is no question that the government is knowingly acquiring Internet transactions that contain wholly domestic communications through its upstream collection."). Read in context, this statement affirmed that, by design rather than accident, the NSA was collecting communications containing tasked selectors—even wholly domestic communications—on the circuits it monitored.

Nothing in this statement or the surrounding analysis, however, suggested that the NSA was collecting *all* such communications. In reviewing the NSA's targeting and minimization procedures, the FISC was concerned with whether the NSA was intentionally acquiring *any* wholly domestic communications. *Id.* at *15–*16; *see also* 50 U.S.C. § 1881a(d)(1)(B). It was not evaluating the comprehensiveness of the NSA's collection practices, *i.e.*, whether the agency was acquiring every last communication "about" a tasked selector or was leaving some communications of interest uncollected because of other restrictions or priorities irrelevant to the question before the FISC. And it did not purport, in this statement, to present a comprehensive description of the NSA's collection procedures.

The Government's traffic-mirroring-with-filtering hypothetical illustrates the point. Both parties agree that, as a technological matter, the NSA would acquire some wholly domestic "about" communications if it applied filters before copying Internet traffic. The Government's concession in the 2011 FISC opinion is thus entirely compatible with the possibility that the NSA filtered out certain categories of Internet traffic before acquiring the wholly domestic transactions discussed. It says nothing about filtering one way or the other, because that stage of the collection process was not the focus of the FISC's analysis. Wikimedia stretches the bounds of inference too far when it reads into the FISC's statement an off-topic proposition not necessarily implied by that statement, and one that would, apparently by accident, reveal state secrets to boot.

Even drawing "all justifiable inferences" in Wikimedia's favor, its out-of-context interpretation of one statement from the 2011 FISC opinion could not support a jury finding in its favor that the NSA actually copies and reviews all communications on a monitored link. *Anderson*, 477 U.S. at 255. And as the majority correctly acknowledges, "Wikimedia's 'grab-bag' of other support" does little to help it bear its burden. Maj. Op. 32. Nor does the excluded portion of Brader's expert report—which is based on speculative assumptions about the NSA's undisclosed surveillance priorities and capabilities—appreciably boost Wikimedia's evidentiary showing. *See*, *e.g.*, *Obama v. Klayman*, 800 F.3d 559, 567 (D.C. Cir. 2015) (Williams, J.) (rejecting the plaintiffs' assertion that the NSA's collection must be comprehensive to be effective because it "rests on an assumption that the NSA prioritizes effectiveness over all other values" and fails to

account for "competing interests that may constrain the government's pursuit of effective surveillance").

The Government's successful assertion of the state secrets privilege erected a significant hurdle for Wikimedia's effort to set forth specific facts showing a genuine dispute on the third prong of the Wikimedia Allegation. I would hold that Wikimedia failed to surmount its burden.