No. 20-1191

IN THE
United States Court of Appeals
for the Fourth Circuit

WIKIMEDIA FOUNDATION,

Plaintiff-Appellant,

v.

NATIONAL SECURITY AGENCY, et al.,

Defendants-Appellees.

On Appeal from the United States District Court for the District of Maryland
Supporting Reversal, Case No. 1:15-cv-00662, Judge T.S. Ellis, III

BRIEF OF CENTER FOR DEMOCRACY & TECHNOLOGY AND NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE AS *AMICI CURIAE* IN SUPPORT OF PLAINTIFF-APPELLANT

Avery W. Gardiner
Gregory T. Nojeim
Mana Azarmi
Stan Adams
CENTER FOR DEMOCRACY & TECHNOLOGY
1401 K Street NW, Suite 200
Washington, D.C. 20005

Sharon Bradford Franklin
Ross Schulman
NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE
740 15th Street NW
Washington, D.C. 20036

Andrew A. Bank
Bret S. Cohen
Allison M. Holt Ryan
Stevie N. DeGroff
HOGAN LOVELLS US LLP
555 Thirteenth Street NW
Washington, D.C. 20004

Counsel for Amici Curiae

Dated: July 8, 2020

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Cases **Page(s)**

Statute

Rule

Other Authorities

International Cases

International Statutes

Other International Authorities

STATEMENT OF INTEREST[1]

The Center for Democracy & Technology ("CDT") is a non-profit public policy organization that works to promote democratic values and constitutional liberties—including free expression, privacy, and open access. In modern times, as new technologies have given governments unprecedented means to access an individual's private information, CDT advocates for the protection of both security and freedom through balanced laws and policies that preserve government accountability and provide meaningful checks on governments' ability to access, collect, and store individuals' private data.

New America's Open Technology Institute ("OTI") works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. New America is a Washington, D.C.-based think tank and civic enterprise committed to renewing American politics, prosperity, and purpose in the "Digital Age." OTI works to ensure that government surveillance is subject to robust safeguards that protect individual rights and provide accountability. This includes promoting transparency for the rules governing the operation of surveillance programs.

[1] All parties have consented to the filing of this brief. Pursuant to Federal Rule of Appellate Procedure 29(a), OTI and CDT each certify that no person or entity, other than OTI or CDT or their counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part.

INTRODUCTION AND SUMMARY OF ARGUMENT

This case raises an important question: Whether the U.S. government's Upstream surveillance[2] under Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), involving the bulk interception of Internet communications, is lawful and constitutional. After several years of litigation before both this Court and the district court, that question has yet to be answered. Instead, the district court's application of the common-law state secrets privilege precluded it from fairly deciding the threshold issue of whether Wikimedia even has Article III standing. Relevant here, the district court entered summary judgment against Wikimedia on the mistaken understanding that the government could not litigate its case without revealing privileged information in its defense. *Wikimedia Found. v.*

[2] Acquisition under Upstream surveillance occurs "with the compelled assistance of providers that control the telecommunications 'backbone' over which telephone and Internet communications transit." Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 7 (July 2, 2014), https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2 (hereinafter, "PCLOB Report"). This includes both "about" communication, which was suspended in 2017, and multiple communications transactions ("MCTs"). *See id*; *see also* Press Release, *NSA Stops Certain 702 "Upstream" Activities*, Nat'l Sec. Agency (April 28, 2017), https://www.nsa.gov/news-features/press-room/Article/1618699/nsa-stops-certain-section-702-upstream-activities/. An MCT is an Internet transaction containing more than one discrete communication within it. "If one of the communications within an MCT is to [or] from . . . a tasked selector, and if one end of the transaction is foreign, the NSA will acquire the entire MCT through upstream collection, including other discrete communications within the MCT that do not contain the selector." PCLOB Report at 7.

Nat'l Sec. Agency/Cent. Sec. Serv., 427 F. Supp. 3d 582, 613 (D. Md. 2019) (JA.7: 4110–11). This is simply not the case. FISA provides specific procedures for judicial review of sensitive information related to electronic surveillance for intelligence purposes, yet the district court deferred wholesale to the government's invocation of the state secrets doctrine. Such unwarranted deference shields the government's surveillance activities—even those that are publicly known—from judicial scrutiny. This is wrong and deprives plaintiffs of their constitutionally mandated day in court.

The government claimed below that a judicial determination regarding Wikimedia's Article III standing would necessarily disclose information about the United States' collection practices that would pose a grave risk to national security. But that argument does not square with reality. As the district court determined, when the government conducts Upstream surveillance, before it ingests any communications into its databases, it first intercepts and scans through communications that transit the Internet backbone. Although the government asserts that Upstream is a targeted surveillance program that ingests only communications to or from specified selectors, it is the government's interception of massive amounts of communications before specific communications are ingested that amounts to bulk surveillance. This broad-scale interception and scanning are the focus of Wikimedia's Fourth Amendment claims in this case.

Moreover, this bulk interception as part of the U.S. government's Upstream surveillance program is similar to the bulk surveillance operations of key U.S. allies and intelligence partners, particularly in Europe. The experiences of these allies demonstrate that it is possible to litigate the legality of bulk interception without compromising national security. Indeed, these governments have made significant disclosures revealing the process and technology employed in bulk cable collection. The capabilities, consequences, and propriety of bulk collection surveillance are disclosed, debated, and litigated openly in other countries.[3] It is therefore difficult to see why bulk interception should be treated so secretly in the United States such that it cannot be challenged in court. Any information revealed by a ruling on Wikimedia's Article III standing pales in comparison to more detailed public disclosures by foreign governments regarding their bulk surveillance programs.

Amici also agree with Appellant that the FISA procedures have displaced the state secrets doctrine in this case. But even if the state secrets privilege were properly invoked below, the district court committed reversible error when

[3] *See* Eric Kind, *Not a Secret: Bulk Interception Practices of Intelligence Agencies*, Ctr. for Democracy & Tech. 38 (Sept. 2019), https://cdt.org/wp-content/uploads/2019/09/2019-09-13-Not-A-Secret-Bulk-Interception-Practices-of-Intelligence-Agencies-FINAL.pdf (hereinafter, "Kind Report") (reviewing government disclosures concerning bulk cable interception globally, and concluding that "[f]ar from being a secret, bulk cable interception is now officially confirmed in a number of countries").

applying it. Dismissal under the state secrets doctrine is a "drastic remedy." *Fitzgerald v. Penthouse Int'l, Ltd.*, 776 F.2d 1236, 1242 (4th Cir. 1985). And the facts here make clear the government has not met the "special burden" necessary "to assure [the Court] that an appropriate balance is struck between protecting national security matters and preserving an open court system." *Abilt v. Cent. Intelligence Agency*, 848 F.3d 305, 311 (4th Cir. 2017) (citation omitted). Because dismissal is only appropriate when "no amount of effort and care on the part of the court and the parties will safeguard privileged material," *Sterling v. Tenet*, 416 F.3d 338, 348 (4th Cir. 2005) (citation omitted), this case should proceed.

Amici understand that security needs require democracies to tolerate a certain amount of secret intelligence surveillance. But that tolerance cannot come at the expense of judicial oversight and reasonable public disclosure. Here, the government cannot be allowed to avoid scrutiny on the theory that the threshold standing inquiry—the consideration of which would require that little, if anything, be revealed about Upstream surveillance beyond what is already publicly acknowledged—poses an unjustifiable risk of grave harm to national security. This Court should reverse and instruct the district court to rule on standing and proceed to the merits.

ARGUMENT

I. OTHER GOVERNMENTS—INCLUDING KEY U.S. ALLIES AND PARTNERS—OPENLY DISCUSS THE CAPABILITIES, CONSEQUENCES, AND LEGALITY OF BULK FIBER OPTIC INTERCEPTION.

The Internet exists as a network of interconnected fiber optic cables.[4] Data is transmitted at different frequencies across the fibers of these cables, allowing each to carry multiple communications channels, or "bearers," at any given time.

To collect data from a cable, a physical probe may be placed on it. To ensure that full communications are identified and collected, it may be necessary to collect data from multiple bearers, fibers, and cables. This is because communications sent over the Internet are first divided into a sequence of smaller pieces of data, called "packets," which are not necessarily transmitted together. For example, a single email, constituting multiple packets, may be sent via different geographic routes, cables, and fibers—and even different bearers within the same fiber. This is one reason why governments like the United Kingdom

[4] *See, e.g.*, *Submarine Cable Map*, TeleGeography, https://www.submarinecablemap.com/ (last visited July 7, 2020). The ownership, length, and landing points of these cables are public information. Cables (and their connection infrastructure) could be owned by any number of entities, including governments, telecommunications companies, or other private companies. The cables themselves are generally made up of combinations of "fibers."

argue that bulk cable interception is necessary: to maximize the chance of identifying, piecing together, and obtaining a sought-after communication.[5]

Governments that conduct bulk cable interception as a form of signals intelligence indicate that they first copy communications in bulk and then use a variety of techniques—including searching for "selectors" or applying "filters"—to sort through the data that has been intercepted in bulk. Specifically, disclosures from the United Kingdom indicate that all communications on an entire given "circuit," or "bearer," are typically copied before they are searched in bulk for selectors. *See infra* Part I.A. Such disclosures are consistent with Wikimedia's expert's opinion that the U.S. government intercepts and copies the entire stream of communications on the international circuits it monitors, irrespective of what selectors they subsequently apply to sort through the intercepted data before ingesting into government databases. *See* Bradner Decl. ¶¶ 368–69 (JA.2: 1058–59).

[5] "United Kingdom's Observations on the Grand Chamber's Questions to the Parties" (hereinafter, "U.K. Observations, May 2019") ¶ 16, *Big Brother Watch v. U.K.,* Application No. 58170/13 (May 2019), https://privacyinternational.org/sites/default/files/2019-07/UK%20Gov%20Obs%20-%20Revised%20Version%20-%20May%202019.PDF ("[S]ince packets associated with a given communication may take different routes to reach their common destination, it may be necessary to intercept all communications over more than one bearer to maximise the chance of identifying and obtaining the communications being sent to [the target].").

The following sections discuss the public oversight and official disclosures regarding bulk cable interception made by other countries.

A. *United Kingdom*

The government of the United Kingdom openly discusses its bulk fiber optic cable interception practices. This informs the public debate about the extent of surveillance in the United Kingdom, as well as the debate in the U.K. Parliament about controls that should be placed on such surveillance. For instance, the U.K. government publishes Fact Sheets regarding its bulk cable interception powers that discuss, among other things, the interception of "large volumes of data" and suggest its program "may incidentally intercept communications of persons who are in the U.K."[6] The United Kingdom also published an "Operational Case for Bulk Powers," in which it described the process of bulk cable interception,[7] and commissioned (and published) an independent review of the use of those "Bulk Powers."[8] Parliament itself

---

[6] U.K. Gov't, *Factsheet - Bulk Interception* (2015), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473751/Factsheet-Bulk_Interception.pdf.

[7] U.K. Gov't, *Operational Case for Bulk Powers* 26–27, 30–33 (2016), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf.

[8] U.K. Parliament, *Independent review of the operational case for bulk powers* (2016), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/527764/TOR for Bulk Review.pdf.

published a report by the Intelligence and Security Committee confirming that U.K. intelligence agencies use "bulk interception techniques [to] access internet communications on a large scale."[9]

The U.K. government also openly discusses bulk cable interception in litigation. For instance, it has provided detailed submissions in ongoing proceedings before the European Court of Human Rights regarding its bulk cable interception program.[10] In these submissions, the United Kingdom admits that it "intercepts communications in 'bulk'—including at the level of communications cables."[11] In addition, the United Kingdom has established a special domestic tribunal—the Investigatory Powers Tribunal—to hear claims against U.K.

[9] Intelligence and Sec. Comm. of U.K. Parliament, *Privacy and Security: A modern and transparent legal framework* 45 (2013), https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf.

[10] *See* U.K. Observations, Dec. 2016; "Further Observations of the Government of the United Kingdom" (hereinafter, "U.K. Further Observations, Dec 2016"), *10 Human Rights Organizations v. United Kingdom*, Application No. 24960/15 (Dec. 2016), https://privacyinternational.org/sites/default/files/2018-02/2016.12.16%20Government%27s%20further%20obs.pdf; "Observations of the Government of the United Kingdom on the Admissibility and Merits of the Application" (hereinafter, "U.K. Observations on Admissibility and Merits, Sept. 2017"), *Big Brother Watch v U.K.*, Application No. 58170/13 (Sept. 2017), https://privacyinternational.org/sites/default/files/2018-02/BBW%26Ors%2C10HROrgs%2CBIJ%26Anr%20-%20Gov%20Observations%20-%202-10-17.pdf.

[11] *See, e.g.*, U.K. Observations, May 2019 ¶ 14.

security and intelligence agencies.[12] That Tribunal has publicly ruled on the lawfulness of particular surveillance activities.[13]

Due to these official statements and court disclosures, the public knows that the United Kingdom employs a bulk cable interception program, which may result in unlawful interception or collection, and understands many of its technological capabilities. This includes a four-step process of bulk cable interception: collection, filtering, "selection for examination," and examination.[14] Critically, with respect to collection, once a bearer is selected, the first step in "accessing" it involves copying the communications and associated data flowing through that bearer.[15] Indeed, the United Kingdom

---

[12] *See* Investigatory Powers Trib., *General Overview and Background* (last updated July 5, 2016), https://www.ipt-uk.com/content.asp?id=10.

[13] *See Liberty & Others vs. the Security Service, SIS, GCHQ* (hereinafter, "*Liberty & Others* (2015)"), IPT/13/77/H (2015), https://www.ipt-uk.com/docs/IPT_13_168-173_H.pdf.

[14] U.K. Observations, May 2019 ¶ 31. The process by which the collected bulk data is sorted and ultimately searched in order to determine which communications to retain, involves filtering and the use of simple and complex queries to comb through the bulk data to select communications with possible intelligence value for further analysis. Of particular relevance here, the U.K. documents highlight that these techniques generally involve first collecting and copying the entire stream of traffic on a circuit or bearer. *See id.* ¶ 29.

[15] *Id.* ¶ 31. The U.K. government also explicitly admits that it selects bearers to access, or copy, on their likely intelligence value, and it undertakes "regular surveys of the contents of bearers: for example, a particular cable might carry a high proportion of communications to or from Syria." U.K. Observations on Admissibility and Merits, Sept. 2017 ¶ 32; *see also* U.K. Observations, May 2019 ¶ 31.

disclosed that, "for technical reasons, it is necessary to intercept the entire contents of a fibre optic cable . . . in order to obtain any intercepted communications or communications data from it at all."[16] The public record also contains details regarding selectors and "complex queries" the U.K. government may use, including various types of queries it runs across the entire contents of an intercepted bearer and the length of time these communications may be stored for examination.[17]

The U.K. government also has publicly argued that—both practically and technologically—its collection ***must be in bulk*** to be effective. In its submissions to the European Court of Human Rights, the United Kingdom described its program in sufficient detail to defend its actions, while maintaining what it considered sufficient secrecy around "the technical details [such as actual selectors]."[18] It further argued that bulk collection and access to "to a substantial volume of communications" is necessary because "electronic communications do not traverse the internet by routes that can necessarily be predicted."[19] Thus, according to the U.K. government, "in order to obtain even a small proportion of

[16] U.K. Observations, May 2019 ¶ 29.

[17] *Id.* ¶¶ 33, 37–45 (describing the "complex query" process); *see also id.* ¶¶ 31–36 (describing further processes).

[18] *Id.* ¶¶ 15–16.

[19] *Id.* ¶ 15.

the communications of known targets overseas, it is necessary for the [Intelligence] Services to intercept a selection of bearers, and to scan the contents of all those bearers for the wanted communications."[20]

Perhaps most important, litigation in the United Kingdom demonstrates that the legality of a particular program of bulk interception can be litigated without endangering national security. For example, ten human rights organizations brought claims in the Investigatory Powers Tribunal related to bulk cable interception, and the Tribunal found that an intelligence agency had unlawfully surveilled two of them.[21] During the litigation, the Tribunal openly discussed the basic parameters of the bulk cable interception program, including that communications were intercepted, filtered, retained, and accessed by an analyst pursuant to U.K. law.[22] Ultimately, the Tribunal found that the communications of two non-profits had been improperly handled, constituting a breach of the non-profits' rights.[23] As a remedy, the Tribunal ordered one copy of the improperly-retained records to be delivered to the Tribunal for potential inspection by the

[20] *Id.*

[21] *Liberty & Others* (2015) ¶ 11.

[22] *Id.* ¶¶ 14–15.

[23] *Id.*

affected party and for any remaining copies to be destroyed.[24] Relevant here, the Tribunal was able to do its work—including identifying the aggrieved parties, ruling on the legality of the retention and handling of information, and redressing violations[25]—without risking grave harm to national security.

B. *Germany*

In Germany, the technological details underpinning bulk cable interception are openly legislated and discussed. Two acts, commonly referred to as the *BND Act* and the *G10 Act*, expressly permit broad monitoring of international telecommunications to identify threats to internal and external security.[26] Together, these two pieces of legislation provide detailed regulation of foreign surveillance, including directly addressing issues of surveilling European Union institutions, member states, and citizens.[27] Further transparency has been provided by the *Bundestag*'s Committee of Inquiry, which held open hearings on the topic of bulk cable interception during which engineers testified about how

[24] *Id*. (also allowing for the government to file "closed," or classified, filings and submissions regarding remedial efforts by the government).

[25] *Id.*

[26] *See* Christian Schaller, *Strategic Surveillance and Extraterritorial Basic Rights Protection: German Intelligence Law After Snowden* (hereinafter, "*Strategic Surveillance*"), 19 German Law Journal 942, 948 nn.38, 39, https://www.cambridge.org/core/services/aop-cambridge-core/content/view/494F82EE78DCF2709B07A2B57D95454C/S2071832200022926a.pdf/strategic_surveillance_and_extraterritorial_basic_rights_protection_german_intelligence_law_after_snowden.pdf.

[27] *Id.* at 943–44.

probes are placed, cables are selected, data is stored before selection, and metadata is processed.[28]

Due to the German government's disclosures, the public record contains a significant amount of detail regarding the technology used for bulk interception. Indeed, the plain text of the German laws contemplates bulk interception, specifically authorizing filters to separate "routine" domestic communications from the communications of foreigners abroad.[29] Entire communications streams are intercepted and screened using filters, and the *G10 Act* requires that applications to use such filters specifically identify the bearer, geographic region, search terms used, and percentage of a communication channel's capacity that will be tapped.[30]

Bulk surveillance has also been the subject of litigation in German courts. A recent decision from the Federal Constitutional Court reviewed the *BND Act* and the *G10 Act* and determined that Germany's Federal Intelligence Service's

---

[28] *See, e.g.*, Witness Statement of Eric Kind ¶ 45, *Privacy International v. Secretary of State for Foreign And Commonwealth Affairs & Others*, Case No. IPT/13/92/CH (19 Jan. 2015), https://privacyinternational.org/sites/default/files/2019-08/2015.01.19%20Eric%20King%20Witness%20statement.pdf.

[29] *See, e.g.*, § 6(1) BND Act; *Strategic Surveillance* at 955–56. To the extent that Germany's bulk interception program collects data not covered by the surveillance laws, "it has to be immediately erased unless there is a separate order for surveillance under the G10 Act." *Strategic Surveillance* at 955.

[30] § 10(4) G10 Act; *Strategic Surveillance* at 957, 979.

surveillance of foreigners in other countries violated the fundamental right to privacy.[31] In its ruling, the Court extensively discussed the German government's surveillance practices, including bulk collection and review of communications, the length of time data can be held and analyzed, the filtering of collected data, and the transferring of unfiltered data to partners.[32] The Court further highlighted the need for independent oversight of surveillance practices to uphold the principle of proportionality in weighing the right to privacy against the effective performance of foreign surveillance.[33] Thus, without revealing information that could do exceptional damage to Germany's national security, the Federal Constitutional Court was able to apply German legal standards to bulk surveillance practices.

C. *Sweden*

In Sweden, bulk interception of fiber optic cables crossing the Swedish border has been openly discussed and debated by the legislature for over a decade.[34] Public oversight and auditing occurs through a panel of judges and

---

[31] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] May 19, 2020, 1 BvR 2835/17, English summary available at https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2020/bvg20-037.html.

[32] *Id.*

[33] *Id.*

[34] *See* Mark Klamberg, *FRA and the European Convention on Human Rights - A Paradigm Shift in Swedish Electronic Surveillance Law,* Overvåking i en Rettstat in the series Nordisk årbok i rettsinformatikk (Nordic Yearbook of Law and Information Technology) 96, 117–18 (2010),

parliamentarians.[35] Sweden has also filed submissions discussing its bulk interception program in the European Court of Human Rights.[36]

As a result of these government disclosures, the public record reflects significant amounts of information regarding Sweden's program. For instance, Sweden has outlined the six stages of its signals intelligence program: (i) identify the signals environment and collect data; (ii) apply automatic collection selectors, or filters, to data; (iii) further process and refine the data (*e.g.*, cryptanalysis, structuring, and language translation); (iv) analyze signals intelligence; (v) disseminate signals intelligence reports; and (vi) provide feedback on use and effect of the signals intelligence.[37] And like the United Kingdom, the Swedish

---

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1558843 (discussing the Swedish Government's introduction of a proposition allowing for various bulk interception in 2006).

[35] "Appendix 1 to the Observations of the Government of Sweden" (hereinafter, "Appendix 1 to Sweden Observations, May 2019") ¶ 123, *Centrum för rättvisa v. Sweden*, Application no. 35252/08, https://cdt.org/wp-content/uploads/2019/09/35252-08-file-35225-08-Annex-1-3-to-GVT-further-OBS.pdf.

[36] *See generally* "Observations of the Government of Sweden" (hereinafter, "Sweden Observations, May 2019"), *Centrum för rättvisa v. Sweden*, Application no. 35252/08, https://centrumforrattvisa.se/wp-content/uploads/2019/07/35252-08file35252_08_GVT_further_OBS_ENG__GC_.pdf.

[37] *See* Appendix 1 to Sweden Observations, May 2019 ¶ 61; *see also* Sweden Observations, May 2019 ¶ 50 (differentiating the "first stage" collection of communications traffic from "the filtering stage (second stage)"). Sweden's *Signals Intelligence Act 2008* explicitly enumerates eight purposes for bulk interception of data entering the country. *See* Appendix 1 to Sweden Observations, May 2019 ¶¶ 50–51 (listing eight purposes as (1) external military threats, (2)

government has disclosed that it believes that data must be intercepted in bulk to provide effective intelligence-gathering.[38]

D. *Other Countries*

Other European countries, including the Netherlands, Finland, and France (and soon, Norway), have laws authorizing bulk cable interception, with each country disclosing varying amounts of information about their practices.[39] Beyond Europe, the South African government has openly discussed bulk surveillance practices. In recent litigation concerning the legality of its bulk interception surveillance program under the National Strategic Intelligence Act, the South African government described bulk surveillance as "an internationally

---

protecting Swedish participation in international peacekeeping or humanitarian missions, (3) prevention against international terrorism and cross-border crimes threatening the national interest, (4) preventing the development or proliferation of weapons of mass destruction, (5) serious external threats to society's infrastructure, (6) foreign conflicts with consequences for international security, (7) foreign intelligence operations against Swedish interests, and (8) counteracting the actions or intentions of a foreign power).

[38] Sweden Observations, May 2019 ¶ 81 (indicating that bulk collection allows the intelligence agencies "to establish a normal communications patterns for reference when detecting anomalies"); *see also* Sweden Observations, May 2019 ¶¶ 49–51, 86 (describing collection and winnowing process on trans-border fiber optic cables).

[39] *See* Kind Report at 33–38; *see also* Norwegian Parliamentary Oversight Comm. on Intelligence and Sec. Servs. *Annual Report 2019*, 13 (March 31, 2020), https://eos-utvalget.no/wp-content/uploads/2020/05/EOS-Committee-annual-report-2019.pdf ("the proposal to introduce facilitated bulk collection [ ] to allow the Norwegian Intelligence Service to collect transboundary electronic communication between Norway and other countries" will be presented to the Norwegian legislature in 2020).

accepted method of strategically monitoring transnational signals" and further explained that "[i]t is basically done through the tapping and recording of transnational signals, including, in some cases, undersea fibre optic cables."[40] Acknowledging the "notorious fact" that "bulk interception[ ] is common practice in many countries," the High Court of South Africa in September 2019 held that South African law does not authorize bulk surveillance.[41] Critically, the court was able to reach the merits of the case in a public court while maintaining the amount of secrecy necessary for the operational details of state surveillance. And in reaching its decision, the court based its analysis on descriptions of the bulk surveillance program provided by the government itself[42] and from other publicly available sources[43]—without requiring additional disclosures that might compromise national security.

These open legislative and judicial regimes reflect a view of governments—including some key U.S. partners and allies—that public courts can review basic

[40] *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* 2019 (1) SA 90 (HC) at 56 ¶ 143 (S. Afr.). The High Court of South Africa noted that this form of monitoring would capture communications between two South Africans in South Africa if the signal passed through a server outside of the country. *Id.* ¶ 145.

[41] *Id.* ¶ 165.

[42] *Id.* ¶ 143.

[43] *Id.* ¶ 144.

information regarding bulk cable interception without jeopardizing national security.

II. DETERMINING ARTICLE III STANDING DOES NOT DISCLOSE STATE SECRETS.

To invoke the state secrets privilege, the government must show that disclosure of a secret will present danger of grave harm to national security. *Abilt*, 848 F.3d at 313 ("the dangers asserted by the government" must be "substantial and real"); *see Doe v. C.I.A.*, 576 F.3d 95, 104 (2d Cir. 2009). Because courts have a "strong interest in allowing otherwise meritorious litigation to go forward," there is a high bar for the application of the state secrets privilege. *Fazaga v. FBI*, 916 F.3d 1202, 1227 (9th Cir. 2019). Courts are charged to critically examine every invocation of the state secrets privilege, *Ellsberg v. Mitchell*, 709 F.2d 51, 58 (D.C. Cir. 1983), and should not abandon judicial control over evidence to the whim of executive officers, *El-Masri v. United States*, 479 F.3d 296, 304 (4th Cir. 2007). "Appropriate judicial oversight is vital to protect against the intolerable abuses that would follow an abandonment of judicial control." *Abilt*, 848 F.3d at 312 (citation and internal quotation marks omitted). Dismissal is appropriate only when no amount of effort or care on the part of the court and parties would safeguard privileged materials. *See Tenet*, 416 F.3d at 348.

Here, *Amici* agree with Appellant that FISA displaces the state secrets privilege in electronic surveillance cases. Rather than simply exclude classified evidence and dismiss the litigation, courts are obligated by Congress to employ *in camera* and *ex parte* procedures to review privileged security information and render decisions based on that information. *See* 50 U.S.C. § 1806(f); *Fazaga*, 916 F.3d at 1232, 1237–38.

Even if the state secrets privilege were not displaced, however, it should not apply here to bar a ruling on Article III standing. Given the significant amount of detail disclosed by other ally and partner governments, this Court should view with skepticism Appellees' contention that a ruling on standing presents a serious risk of grave harm to national security. Finding that Wikimedia's communications were intercepted does not, as the district court reasoned, require the harmful disclosure of protected state secrets. Rather, it would merely make known that one of Wikimedia's near-ubiquitous communications was intercepted in the first stage of the U.S. government's Upstream surveillance program. Such a determination would not reveal—and indeed does not depend on—whether Wikimedia's communications were actually ingested into the government's databases. Nor would it expose any detailed information about the methods of the Upstream surveillance program, or the government's scanning and ingestion practices. Nor would it reveal technological capabilities, retention, examination, specific targets,

investigations, or other actually sensitive information. Put simply, a ruling on standing would reveal much less information about bulk surveillance than other governments—including U.S. allies and partners—publicly discuss, debate, and litigate.

As foreign courts have shown, state surveillance practices can be fairly litigated without harmful public revelations of privileged national security information. And to the extent the district court believes national security is truly at stake or that it must conduct a preliminary review of privileged information the government may provide in its defense, it should employ FISA procedures. At bottom, the district court cannot altogether refuse to rule on Article III standing and thwart any judicial review of the legality of the bulk interception stage of Upstream collection.

CONCLUSION

The open discussion of bulk cable interception by officials and/or courts in the United Kingdom, Germany, Sweden, and South Africa, among other countries, clearly refutes the U.S. government's insistence that a ruling on standing presents a grave risk to national security. To accept this argument is to shield broad-scale government surveillance from judicial review, even when the government need not reveal any details regarding operation of Upstream surveillance in order to assess Wikimedia's claims. To the extent any

information is truly sensitive enough to shield it from Appellant or the public, Congress provided special mechanisms in FISA to allow the district court to evaluate the legality of the surveillance without risking disclosure. There is no reason for the district court to refrain from fairly evaluating and ruling on Wikimedia's Article III standing, and subsequently reaching the legality and constitutionality of the government's Upstream surveillance program. This Court should reverse.

July 8, 2020

Respectfully submitted,

/s/ Andrew A. Bank

Andrew A. Bank
Bret S. Cohen
Allison M. Holt Ryan
Stevie N. DeGroff
HOGAN LOVELLS US LLP
555 Thirteenth Street NW
Washington, D.C. 20004

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7) and Fed. R. App. 29(a)(5) because this brief contains 4,707 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Office Word in Times New Roman 14-point type.

/s/ Andrew A. Bank

Andrew A. Bank
HOGAN LOVELLS US LLP
555 Thirteenth Street NW
Washington, D.C. 20004
(202) 637-5600
andrew.bank@hoganlovells.com

Dated: July 8, 2020

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing on July 8, 2020. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

/s/ Andrew A. Bank
Andrew A. Bank
HOGAN LOVELLS US LLP
555 Thirteenth Street NW
Washington, D.C. 20004
(202) 637-5600
andrew.bank@hoganlovells.com

Dated: July 8, 2020