No. 19-16066

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

CAROLYN JEWEL *et al.*,
Plaintiffs-Appellants,

v.

NATIONAL SECURITY AGENCY *et al.*,
Defendants-Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA
NO. 4:08-CV-04373-JSW
The Honorable Jeffrey S. White, District Court Judge

BRIEF OF CENTER FOR DEMOCRACY AND TECHNOLOGY AND NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE AS *AMICI CURIAE* IN SUPPORT OF PLAINTIFFS-APPELLANTS AND IN SUPPORT OF REVERSAL

[All Parties Have Consented. FRAP 29(a)]

Victor Jih
Conor Tucker
IRELL & MANELLA LLP
1800 Avenue of the Stars, Suite 900
Los Angeles, CA 90067-4276
(310) 277-1010
Attorneys for Amici Curiae

Lisa A. Hayes
Gregory T. Nojeim
CENTER FOR DEMOCRACY & TECHNOLOGY
1401 K Street NW, Suite 200
Washington, D.C. 20005
(202) 637-9800

Ross Schulman
NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE
740 15th St. NW
Washington, DC 20005
(202) 986-0427

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *Amici Curiae* Center for Democracy and Technology and New America's Open Technology Institute state that neither have parent corporations and that no publicly held corporation owns 10% or more of either of their stock.

STATEMENT OF INTEREST[1]

The Center for Democracy and 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 when 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, DC-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] Pursuant to Federal Rule of Appellate Procedure 29(a), OTI certifies that no person or entity, other than OTI, its members, or its counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part. CDT certifies that the Open Society Foundations supported CDT's work on the brief. All parties consent to the filing of this brief.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTRODUCTION AND SUMMARY OF ARGUMENT

This case raises the important question of whether mass surveillance by the United States government through the bulk interception of Internet communications and telephone records is lawful and constitutional. After 11 years of litigation, that question has yet to be answered. Instead, the district court held most recently that the state secrets doctrine precludes it from deciding even the threshold issue of whether these plaintiffs have standing. The district court made this determination after finding it "owe[d] significant deference" to the Executive branch such that "even a simple 'yea or nay' … would do grave harm to national security." ER026. Although the Foreign Intelligence Surveillance Act (FISA) provides specific procedures for judicial review of the legality of electronic surveillance engaged in for intelligence purposes—*e.g.*, 18 U.S.C. § 1806(f)—the district court instead deferred to the Executive's invocation of the state secrets doctrine to shield the Executive's own surveillance activities from judicial scrutiny. This is not the correct result.

Amici understand that security needs may require that democracies tolerate a certain amount of secret intelligence surveillance. But that tolerance cannot come at the expense of judicial oversight. Indeed, Congress has explicitly provided for judicial oversight of electronic surveillance through the FISA procedures. *Amici* agree with Appellants that these procedures have displaced the state secrets

doctrine in this case. As a result, the state secrets privilege provides no basis to dismiss this case and the district court committed reversible error when it refused to reach the merits.

But even if the state secrets doctrine applied, the district court committed reversible error when applying it. The district court abandoned judicial review in the name of national security. Because of the possibility of such "drastic result[s]," relief in the form of dismissal under the state secrets doctrine "should not be readily granted." *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1089 (9th Cir. 2010). Rather than "owe deference" to the Executive—as the district court felt obligated to do—this Court has recognized that the doctrine imposes a "special burden" on district courts to strike a balance between "protecting national security matters and preserving an open court system." *Al-Haramain Islamic Found., Inc. v. Bush*, 507 F.3d 1190, 1203 (9th Cir. 2007). Only where "unacceptable" or "unjustifiable" risk of disclosure would work "grave harm to national security" may a district court abandon judicial review. *Jeppesen*, 614 F.3d at 1087, 1090. The Government has not met that high bar in this case.

The Government claimed that a court determination as to whether the plaintiffs had standing would necessarily disclose information about its bulk interception practices that would pose a grave risk to U.S. national security. The district court's acceptance of that argument is particularly difficult to understand

given that it is hardly a secret that governments intercept communications travelling across fiber optic communication cables, in bulk, to support their signal intelligence programs. Governments have acknowledged these programs. Many have gone further and have disclosed the methods used in bulk interception. This surveillance—including capabilities, consequences, and propriety—is openly and in detail discussed in Europe. CDT has recently issued a report that discusses government disclosures concerning bulk cable interception. *See* Eric Kind, "Not a Secret: Bulk Interception Practices of Intelligence Agencies" *available at* https://cdt.org/insight/not-a-secret-bulk-interception-practices-of-intelligence-agencies/ (hereinafter "Kind Report").

Key U.S. allies and intelligence partners, particularly in Europe, have made significant disclosures regarding the process and technology of bulk cable interception. Given these disclosures, it is hard to see why bulk interception needs to be treated so secretly in the United States that it cannot be challenged in court—especially given the *in camera* and *ex parte* FISA procedures that enable the district court to evaluate classified materials and issue classified rulings. A simple "yea or nay" on standing does not disclose any meaningful detail about the government's surveillance program: not whether the intercepted communications were one or many, not whether the collection was direct or inadvertent, not where a copy of the communication may have been found, and not any other detail that

might provide foreign enemies actionable information about U.S. surveillance activities. Indeed, any information revealed by ruling on standing pales in comparison to the much more detailed disclosures other governments make regarding bulk cable interception programs.

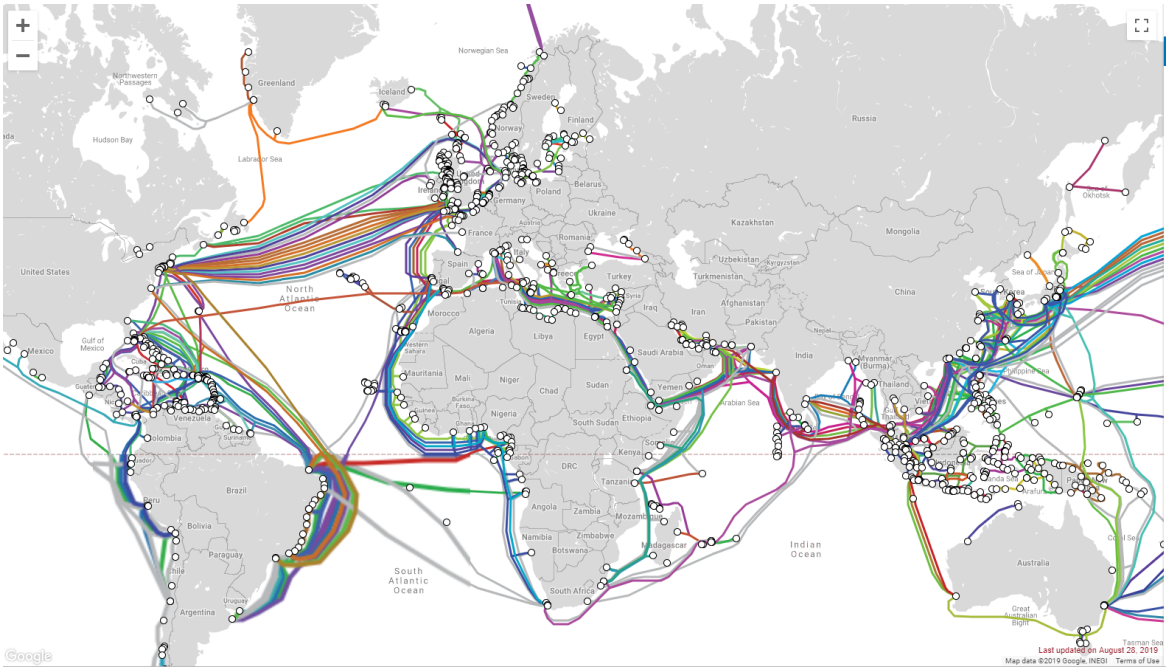
The U.S. Government cannot be allowed avoid scrutiny of its actions on a theory that a threshold ruling on standing poses unjustifiable risk of grave harm to national security. As the European examples indicate, discussion, debate, and even litigation regarding the legality of bulk interception is possible. This Court should reverse and instruct the District Court to rule on standing and proceed to the merits.

ARGUMENT

I. EUROPEAN GOVERNMENTS OPENLY DISCUSS BULK FIBER OPTIC INTERCEPTION, INCLUDING ITS CAPABILITIES, CONSEQUENCES, AND LEGALITY.

To understand the richness of public knowledge about bulk cable interception practices around the world, it is first necessary to understand how communications are transmitted across the internet. The internet exists as a

network of interconnected fiber optic cables, many of which are on the sea floor. *See, e.g.*, http://www.submarinecablemap.com *last accessed* Sept. 5, 2019.



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 (such as AT&T), or other private companies. The cables themselves are generally made up of combinations of "fibers." Data is transmitted through these fibers as light. By transmitting light at different frequencies, each fiber is able to carry multiple communications channels, or "bearers," at once.

To collect data from a cable, a physical probe may be placed on it. To make sure 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, such as emails, are first split into separate components, or "packets" and these packets are not necessarily transmitted together. A single email, constituting multiple packets, may often be sent via different geographic routes, different cables, different fibers, and even different bearers within the same fiber. This is one reason why governments like the United Kingdom argue that bulk cable interception is necessary: to maximize the chance of identifying, piecing together and obtaining a sought-after communications.[2]

Governments who conduct bulk cable interception as a form of signals intelligence indicate that they use filters to sort through the intercepted data. While there are many types of filters, they are most easily categorized into two sets: negative filters and positive filters. A negative filter identifies material to immediately discard. An example might be: "automatically discard all streaming video data identified as Netflix." A positive filter is used to identify material to retain. An example might be: "automatically retain information to or from so-and-

[2] "[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]." 'United Kingdom's Observations on the Grand Chamber's Questions to the Parties', at § 16, *Big Brother Watch v. U.K.* (May 2019), (Application No. 58170/13), available at: https://privacyinternational.org/sites/default/files/2019-07/UK%20Gov%20Obs%20-%20Revised%20Version%20-%20May%202019.PDF (hereinafter U.K. Observations, May 2019).

so@domain.com." Both types of filters can be extraordinarily complex and many countries have explicit rules or laws governing the use of these filters.

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

A. The United Kingdom

The government of the United Kingdom ("U.K.") openly and publicly discusses its bulk fiber optic cable interception practices. For instance, the U.K. publishes Fact Sheets regarding its bulk cable interception powers, which discuss—among other things—interception of "large volumes of data" and that indicate its program "may incidentally intercept communications of persons who are in the U.K."[3] The authorities underlying the U.K.'s bulk cable interception powers are openly legislated and debated; and its use is audited. The U.K. published an "Operational Case for Bulk Powers," in which it described the process of bulk cable interception.[4] The U.K. also commissioned (and published) an independent review of the use of those "Bulk Powers."[5] Parliament itself has

---

[3] *"Factsheet - Bulk Interception,"* U.K. Government (2015) available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473751/Factsheet-Bulk_Interception.pdf.

[4] *'Operational case for Bulk Powers'* pp. 26-27, 30-33, U.K. Government, (2016), available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf.

[5] *'Independent review of the operational case for bulk powers',* U.K. Parliament, (2016), available at:

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."[6] Further, "bulk interception warrants" are written into the *Investigatory Powers Act of 2016*.[7]

The U.K. government also openly discusses bulk cable interception in litigation. For instance, the U.K. has provided detailed submissions in ongoing proceedings before the European Court of Human Rights regarding its bulk cable interception program.[8] In these submissions, the U.K. admits that it "intercepts

---

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/527764/TOR_for_Bulk_Review.pdf.

[6] 'Privacy and Security: A modern and transparent legal framework' at 6, The Intelligence and Security Committee of Parliament (2013) available at: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf.

[7] § Chapter 1, *Investigatory Powers Act 2016 available at* http://www.legislation.gov.uk/ukpga/2016/25/contents.

[8] U.K. Observations, May 2019; 'Further Observations of the Government of the United Kingdom', *10 Human Rights Organizations v. United Kingdom Application No. 24960/15*, (Dec 2016) available at: https://privacyinternational.org/sites/default/files/2018-02/2016.12.16%20Government%27s%20further%20obs.pdf (hereinafter U.K. Further Observations, Dec 2016); 'Observations of the Government of the United Kingdom on the Admissibility and Merits of the Application', Big Brother Watch v U.K. Application No. 58170/13, (Sept 2017) available at: https://privacyinternational.org/sites/default/files/2018-02/BBW%26Ors%2C10HROrgs%2CBIJ%26Anr%20-%20Gov%20Observations%20-%202-10-17.pdf (hereinafter U.K. Observations on Admissibility and Merits, Sept. 2017).

communications in 'bulk' – including at the level of communications cables."[9] Additionally, the U.K. has established a special domestic tribunal—the Investigatory Powers Tribunal—to hear claims against U.K. security and intelligence agencies.[10] That Tribunal has publicly ruled on the lawfulness of particular surveillance activities.[11]

Because of these government statements, the public knows that its government employs a bulk cable interception program (which can inadvertently or intentionally result in unlawful interception or collection) as well as many of its technological capabilities. For instance, the U.K. government has discussed and described the four-step process of bulk cable interception as a part of its signal intelligence network: collection, filtering, 'selection for examination,' and examination.[12] The U.K. also explicitly admits 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."[13] Additionally, the public record contains details regarding positive filters the U.K. government may use, including

---

[9] *See, e.g.*, U.K. Observations, May 2019.
[10] *See* The Investigatory Powers Tribunal, General Overview and Background, https://www.ipt-uk.com/content.asp?id=10.
[11] *See Liberty & Others vs. the Security Service, SIS*, GCHQ IPT/13/77/H (2015) available at: https://www.ipt-uk.com/docs/Final_Liberty_Ors_Open_Determination_Amended.pdf (hereinafter "Liberty & Others (2015)").
[12] § 31 U.K. Observations, May 2019.
[13] § 32 U.K. Observations on Admissibility and Merits, Sept. 2017.

the 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.[14] The U.K. government has discussed in detail its own "complex queries," which include "searching for material which combined use of a particular language, emanation from a particular geographic region, and use of a specific technology" or using "a complex digital signature created by a particular machine used in cyber attacks."[15] The U.K. government has even discussed techniques for selecting which bearers to intercept, revealing that it uses machine learning to facilitate the process.[16]

In addition, because of ongoing litigation in the European Court of Human Rights, we also know that the U.K. government's position is that—both practically and technologically—the collection must be ***in bulk***. In its submissions to the court, the U.K. government 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, which] are sensitive."[17] Practically, the U.K. government argues that without bulk collection the tool would be ineffective.

---

[14] §§ 33, 37-45 U.K. Observations, May 2019 (describing the "complex query" process); *see also* §§ 32-36 (describing further processes).
[15] § U.K. Observations, May 2019.
[16] *See* David Bond, *Inside GCHQ: The Art of Spying in the Digital Age*, Financial Times, May 22, 2019 , *available at:* https://www.ft.com/content/ccc68ffc-7c1e-11e9-81d2-f785092ab560.
[17] § 15 U.K. Observations, May 2019.

In order to conduct targeted searches, the U.K. claims that "the [Intelligence] Services [must] have access to a substantial volume of communications through which to search for links."[18] The U.K. government argues that bulk collection is necessary because "electronic communications do not traverse the internet by routes that can necessarily be predicted."[19] Thus, according to the U.K.:

> in order to obtain even a small proportion of 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 importantly, the U.K. example demonstrates that the legality of a particular program of bulk cable interception can be litigated without endangering national security. For instance, 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] In the course of the litigation, the Tribunal openly discussed the basic parameters of U.K.'s bulk cable interception program, including that communications were intercepted, filtered, retained, and accessed by an analyst pursuant to U.K. law.[22] However, the communications of two non-profits

---

[18] § 15 U.K. Observations, May 2019.
[19] §§ 15-16 U.K. Observations, May 2019.
[20] § 15 U.K. Observations, May 2019.
[21] Liberty & Others (2015) § 10.
[22] *Id.* §§ 7-11, 14-15.

had been retained beyond the limit permitted by U.K. law or were 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 affected party) and for any remaining copies to be destroyed.[24] 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 unjustifiably risking grave harm to national security.

B. Sweden

In Sweden, bulk interception of fiber optic cables crossing the Swedish border has been openly discussed for over a decade. It has been debated by the legislature since 2006.[26] Public oversight and auditing occurs through a panel of

---

[23] *Id.* §§ 14-15.
[24] *Id.* §§ 14-15 (also allowing for the government to file "closed," i.e., classified, filings and submissions regarding remedial efforts by the Government).
[25] §§ 14-15 Liberty & Others (2015).
[26] *See* Mark Klamberg, "FRA and the European Convention on Human Rights - A Paradigm Shift in Swedish Electronic Surveillance Law" at pp. 117-18 in Dag Wiese Schartaum (ed.) 'Overvåking i en Rettstat' in the series Nordisk årbok i rettsinformatikk (Nordic Yearbook of Law and Information Technology), pp. 96-134, Fagforlaget, Bergen (2010) *available at* 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 available at https://www.regeringen.se/rattsliga-dokument/proposition/2007/03/prop.-20060763/).

judges and parliamentarians.[27] Sweden has also filed submissions discussing its bulk interception program in the European Court of Human Rights.[28]

Because of these government disclosures, the public record reflects significant amounts of information regarding Sweden's program. For instance, the stages of the bulk cable interception process are disclosed and include: (1) identification and extraction; (2) automatic collection selectors; (3) further refinement (including translation); (4) analysis; (5) disseminating report; (6) feedback.[29] Indeed, the Swedish *Signals Intelligence Act 2008* even explicitly enumerates eight purposes for bulk interception of data entering the country.[30]

---

[27] § 123 'Appendix 1 to the Observations of the Government of Sweden', Centrum för rättvisa v. Sweden Application no. 35252/08, available at: https://cdt.org/files/2019/09/35252-08-file-35225-08-Annex-1-3-to-GVT-further-OBS.pdf (hereinafter Appendix 1 to Sweden Observations, May 2019).

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

[29] §3.4.44 Appendix 1 to Sweden Observations, May 2019.

[30] "[T]he Government would like to point to the fact that signals intelligence conducted on fiber-optic cables may only concern communications crossing the Swedish border in cables owned by a network operator." Sweden Observations, May 2019; *see* § 1 Signals Intelligence Act (2008:717) at Appendix 6 to Sweden Observations, May 2019 *available at* https://cdt.org/files/2019/09/14-e-GOVT-Annex-6.pdf (listing eight purposes as: 1) external military threats, 2) 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

Like the U.K., the Swedish government has disclosed that it believes that data must be intercepted in bulk to provide effective intelligence-gathering.[31] In addition, the public record includes indications of the Swedish government's technological capacity to target specific bearers within a fiber, as warrants are ***required by law*** to specify specific bearers.[32] Importantly, the public is aware that network operators cooperate in the program, since they are required by law to facilitate interception.[33] And, while content of specific "permits" are not discussed openly, the length of permits is publicly avowed (renewable six month durations, with some in place for several years).[34]

C. 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*, were reformed in the wake of leaks about intelligence

---

operations against Swedish interests, and 8) counteracting the actions or intentions of a foreign power.).

[31] § 81 Sweden Observations, May 2019 (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).

[32] § 75 Appendix 1 to Sweden Observations, May 2019.

[33] §§ 42-43, 61 Appendix 1 to Sweden Observations, May 2019. This corporation must be in such a manner that the surveillance is not disclosed to third parties. *Id.* §§ 42-43.

[34] § 27 Sweden Observations, May 2019.

surveillance that were made in 2013 by former NSA contractor Edward Snowden. This legislation explicitly allows for broad monitoring of international telecommunications to identify threats to internal and external security.[35] Together, the two acts constitute extremely detailed regulation of foreign surveillance, including directly addressing issues of surveilling European Union institutions, member states, and citizens.[36] In addition, both acts create mechanisms to review surveillance measures, including, under the *G10 Act*, jurisdiction over the processing and use of personal data.[37] Further transparency has been provided by the *Bundestag*'s Committee of Inquiry, which held open hearings on the topic of bulk cable interception.

---

[35] For *BND Act*: *see* Christian Schaller, 'Strategic Surveillance and Extraterritorial Basic Rights Protection: German Intelligence Law After Snowden,' German Law Journal Vol. 19 No. 04 at 948 n.39 *available at*: 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 (hereinafter *Strategic Surveillance*) ("Gesetz über den Bundesnachrichtendienst [BND-Gesetz, BNDG] [Federal Intelligence Service Act] [BND Act], Dec. 20, 1990, BGBL. I at 2954, 2979, last amended by Gesetz [G], June 30, 2017 BGBL. I at 2097 (Ger.)."). For *G10 Act*: *see id.* at 948 n. 38 ("Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses [Artikel-10 Gesetz, G 10] [Act on Restricting the Privacy of Correspondence, Posts, and Telecommunications] [G10 Act], June 26, 2001, BGBL. I at 1254, 2298, last amended by Gesetz [G], Aug. 14, 2017 BGBL. I at 3202 (Ger.)").

[36] *Strategic Surveillance* at 943-44. .

[37] § 15 *G10 Act*; § 16 *BND Act*; *see Strategic Surveillance* at 954, 958.

Because of these government disclosures, the public record contains a significant amount of detail regarding the technology used for bulk interception. For instance, the plain text of the German laws acknowledge that bulk interception is contemplated by specifically providing for the application of specialized (and detailed) filters to sort out protected data.[38] The *G10 Act* requires that applications for authorization must specifically identify the bearer as well as the percentage of a communication channel's capacity which will be tapped.[39] The laws provide explicit indications of the capacities of Germany's filter system, as (under the *G10 Act*) search terms and geographic region must be expressly listed in applications for authorization.[40] Furthermore, public hearings featured testimony of engineers regarding how probes are placed, how they undertake cable selection, how data is stored before selection, and the processing of metadata (*i.e.*, data about the communications apart from the communications themselves).[41] The Committee's

---

[38] *See, e.g.*, § 6(1) *BND Act*; *Strategic Surveillance* at 955-56.
[39] § 10(4) *G10 Act*; *Strategic Surveillance* at 958, 978.
[40] § 10(4) *G10 Act*; *Strategic Surveillance* at 958, 978.
[41] *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) *available at* https://privacyinternational.org/sites/default/files/2019-08/2015.01.19%20Eric%20King%20Witness%20statement.pdf; for full discussion in German, *see* Meister, 'Live blog from the intelligence committee of inquiry', *Netzpolitik*, (Nov. 2014) available at: https://netzpolitik.org/2014/live-blog-aus-dem-geheimdienst-untersuchungsausschuss-bnd-mitarbeiter-k-l-und-p-auf-der-zeugebank/.

Report, currently available only in German, publicly discusses the work of the inquiry.[42] Thus, the public has a tremendous amount of information regarding Germany's program.

D. Other Countries

Other countries, including the Netherlands, Finland, France, and (soon) Norway have legislation authorizing bulk cable interception—with each country disclosing various amounts of information about their practices. *See* Kind Report at 33-38. These open legislative regimes reflect a view of governments—including by some that key partners and allies of the United States—that national security does not require complete silence regarding bulk cable interception.

II. IN LIGHT OF THE FOREGOING, SIMPLY DECIDING PLAINTIFFS' 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 v. Central Intelligence Agency*, 848 F.3d 305, 313 (4th Cir. 2017) (the privilege extends only where "the dangers asserted by the government are substantial and real"); *Doe v. C.I.A.*, 576 F.3d 95, 104 (2d Cir. 2009) ("The district court must …

[42] 'Committee of Inquiry report into mass surveillance', German parliament (2017) https://dipbt.bundestag.de/doc/btd/18/128/1812850.pdf; *see also* Dissenting Committee of Inquiry report available semi-officially at: https://cdn.netzpolitik.org/wp-upload/2017/06/2017-06-20_NSAUA-Sondervotum-Opposition-geschwaerzt.pdf.

satisfy[] itself that there is a reasonable danger that disclosure of the particular facts in litigation will jeopardize national security.”). If applicable, the privilege can bar consideration of the secret or even adjudication of a matter in its entirety.

Because courts have a "strong interest in allowing otherwise meritorious litigation to go forward," this Court has set the bar high for application of the states secret privilege. *Fazaga v. FBI*, 916 F.3d 1202, 1227 (9th Cir. 2019). The state secrets privilege has "drastic result[s] and should not be readily granted." *Jeppesen*, 614 F.3d at 1089; *see also Fazaga*, 916 F.3d at 1227. Indeed, the privilege imposes "a special burden" on courts to strike the "appropriate balance … between protecting national security matters and preserving an open court system." *Al-Haramain*, 507 F.3d at 1203. The privilege must be limited to instances in which the court is satisfied that the risk of disclosure is "unacceptable" or "unjustifiable" and would work "grave harm to national security." *Jeppesen*, 614 F.3d at 1090. This is a high bar.

Amici agree with appellants that FISA displaces the state secrets privilege in electronic surveillance cases. Instead of excluding classified evidence or dismissing litigation, Congress authorized *in camera* and *ex parte* procedures to review state secrets 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 was not displaced, however, it should not apply here to prevent a ruling on standing. Given the enormous amount of detail disclosed by other governments, the Court should view with skepticism the U.S. Government's contention that a ruling on standing presents a serious risk of grave harm to national security. Finding that at least one of plaintiff's communications were intercepted does not, as the district court claimed, reveal the "specific nature and operational details of the process and scope of" the bulk interception. ER021. Such a holding would reveal next to nothing about methods, maximum technological capabilities, retention, examination, targets, investigations, or other arguably sensitive information. Indeed, a ruling on standing would reveal much less information than other governments publicly discuss, debate, and litigate. To the extent the district court believes national security is truly at stake, it can use the FISA procedures. But the district court cannot altogether refused to rule on standing and prevent any judicial review of the legality of the bulk interception.

CONCLUSION

When compared to its European countries (including many allies), the United States already errs too much on the side of secrecy at the expense of judicial review. While courts in allied countries openly litigate the lawfulness of bulk cable interception activities, the U.S. government insists that such litigation in the U.S. must be dismissed because any discussion about any aspect of its bulk

interception program jeopardizes national security. To accept this argument is to leave potentially unlawful and unconstitutional bulk interception regimes in place without judicial review.

The open discussion of bulk cable interception by officials in the U.K., Germany, Sweden, and other countries, makes it clear that such absolute secrecy about surveillance practices of the U.S. Government is not necessary to protect national security. Given how freely this interception is discussed by others, the U.S. Government must be pressed hard to explain how a ruling on standing presents an serious and grave risk to national security.

To the extent any information is truly secret, Congress provided special procedures in FISA to allow the district court to rule on the legality of the surveillance without their disclosure. There was thus no reason for the district court to refrain from ruling on Appellants' standing and reaching the legality and constitutionality of the interception program. This Court should reverse.

Dated: September 13, 2019

Respectfully submitted,

IRELL & MANELLA LLP

By: */s/ Victor Jih*
Victor Jih
Attorneys for Center for Democracy and Technology and New America's Open Technology Institute

CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing Brief of Center for Democracy and Technology and New America's Open Technology Institute as *Amici* Curiae in Support of Plaintiffs-Appellants complies with the type-volume limitations of the Federal Rules of Appellate Procedure. Exclusive of the items identified in Federal Rule of Appellate Procedure 32(f), the brief contains 4,270 words. The brief was prepared using Microsoft Word 2016. The undersigned has relied upon the word count feature of this word processing system in preparing this certificate.

Dated: September 13, 2019

IRELL & MANELLA LLP

By: */s/ Conor Tucker*
Conor Tucker

CERTIFICATE OF SERVICE

I hereby certify that on September 13, 2019, the foregoing was electronically filed with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit using the Court's CM/ECF system which will serve all participants.

Dated: September 13, 2019

IRELL & MANELLA LLP

By: */s/ Victor Jih*
Victor Jih