No. _____

# In The
# Supreme Court of the United States

CAROLYN JEWEL, TASH HEPTING, ERIK KNUTZEN, YOUNG BOON HICKS (AS EXECUTRIX OF THE ESTATE OF GREGORY HICKS), AND JOICE WALTON,

*Petitioners,*

v.

NATIONAL SECURITY AGENCY, ET AL.,

*Respondents.*

**On Petition For Writ Of Certiorari To The United States Court Of Appeals For The Ninth Circuit**

## PETITION FOR A WRIT OF CERTIORARI


THOMAS E. MOORE III
HAYNES AND BOONE, LLP
525 University Avenue
Suite 400
Palo Alto, CA 94301
Telephone: (650) 687-8800

RACHAEL E. MENY
BENJAMIN W. BERKOWITZ
KEKER, VAN NEST & PETERS LLP
633 Battery Street
San Francisco, CA 94111
Telephone: (415) 391-5400

ARAM ANTARAMIAN
LAW OFFICE OF ARAM ANTARAMIAN
1714 Blake Street
Berkeley, CA 94703
Telephone: (510) 841-2369

RICHARD R. WIEBE
*Counsel of Record*
LAW OFFICE OF RICHARD R. WIEBE
44 Montgomery Street
Suite 650
San Francisco, CA 94104
Telephone: (415) 433-3200
wiebe@pacbell.net

CINDY A. COHN
DAVID GREENE
LEE TIEN
KURT OPSAHL
ANDREW CROCKER
AARON MACKEY
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333

*Counsel for Petitioners*



COCKLE LEGAL BRIEFS (800) 225-6964
WWW.COCKLELEGALBRIEFS.COM

## QUESTIONS PRESENTED

This lawsuit challenges publicly-acknowledged government mass-surveillance programs that over the past 20 years have (1) intercepted, copied, and searched the Internet communications, and (2) collected and searched the phone records, of hundreds of millions of innocent Americans. The district court, however, excluded under the state-secrets privilege public evidence showing that the mass surveillance included petitioners' communications and communications records; it held that 50 U.S.C. § 1806(f)'s procedures for using secret evidence in electronic-surveillance lawsuits did not displace the state-secrets privilege; and it dismissed petitioners' claims under the state-secrets privilege as nonjusticiable. The Ninth Circuit affirmed in a cursory three-page decision. In addition to its public dismissal order, the district court issued a classified order never disclosed to petitioners adjudicating their standing using secret evidence the court ordered the government to produce pursuant to section 1806(f) and 18 U.S.C. § 2712(b)(4). The Ninth Circuit did not adjudicate petitioners' appeal of the classified order.

This petition presents the following questions closely intertwined with the issues pending before the Court in *U.S. v. Abu Zubaydah*, No. 20-827, and *FBI v. Fazaga*, No. 20-828.

1. May a district court use the state-secrets privilege to exclude public evidence establishing a plaintiff's standing to challenge government mass

**QUESTIONS PRESENTED**—Continued

surveillance and then dismiss the action under the state-secrets privilege as nonjusticiable?

2. When pursuant to 18 U.S.C. § 2712(b)(4) and 50 U.S.C. § 1806(f) a district court has granted a plaintiff's discovery motion seeking evidence relating to electronic surveillance and the government produces the evidence to the court *in camera* and *ex parte*, may the plaintiff rely on that secret evidence to establish her standing or may the district court instead dismiss the action under the state-secrets privilege as nonjusticiable?

3. On appeal, may a court of appeals refuse to review for error a district court's classified dispositive order never disclosed to the plaintiff-appellant?

## PARTIES

Plaintiffs and petitioners are Carolyn Jewel, Tash Hepting, Erik Knutzen, Young Boon Hicks (as executrix of the estate of Gregory Hicks), and Joice Walton. They bring their claims individually and, for their Fourth Amendment claims, as representatives of a putative injunctive-relief-only class comprising AT&T's customers.

Defendants and respondents are the National Security Agency (NSA); NSA Director General Paul Nakasone, in his official capacity; Keith B. Alexander, former NSA Director, in his personal capacity; Michael V. Hayden, former NSA Director, in his personal capacity; the United States of America; President Joseph Biden, in his official capacity; former President George W. Bush, in his personal capacity; former Vice-President Richard B. Cheney, in his personal capacity; David S. Addington, in his personal capacity; Department of Justice; Attorney General Merrick Garland, in his official capacity; former Attorney General Michael B. Mukasey, in his personal capacity; former Attorney General Alberto R. Gonzales, in his personal capacity; former Attorney General John D. Ashcroft, in his personal capacity; Avril Haines, Director of National Intelligence (DNI), in her official capacity; former DNI John M. McConnell, in his personal capacity; and former DNI John D. Negroponte, in his personal capacity.

## RELATED PROCEEDINGS

*Jewel v. NSA*, No. 08-CV-04373-JSW, U.S. District Court for the Northern District of California. Judgment entered Apr. 25, 2019.

*Jewel v. NSA*, No. 19-16066, U.S. Court of Appeals for the Ninth Circuit. Judgment entered Aug. 17, 2021.

TABLE OF CONTENTS

TABLE OF CONTENTS—Continued

TABLE OF CONTENTS—Continued



APPENDIX

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

## PETITION FOR A WRIT OF CERTIORARI

Petitioners Carolyn Jewel, Tash Hepting, Erik Knutzen, Young Boon Hicks (as executrix of the estate of Gregory Hicks), and Joice Walton respectfully petition for a writ of certiorari to review the judgment of the United States Court of Appeals for the Ninth Circuit.

## DECISIONS BELOW

The district court's public opinion is at 2019 WL 11504877 (N.D. Cal. Apr. 25, 2019).

The district court's classified opinion, never disclosed to petitioners, is available from the Litigation Security Group of the Department of Justice. *See* Petition Appendix ("App.") 45a.

The court of appeals' decision is at 2021 WL 3630222 (9th Cir. Aug. 17, 2021).

## JURISDICTION

The Ninth Circuit entered judgment August 17, 2021, and denied rehearing October 26, 2021.

This Court has jurisdiction under 28 U.S.C. § 1254(1).

## RELEVANT STATUTORY PROVISIONS

The relevant statutory provisions, set forth in the appendix, are 18 U.S.C. § 2712 and 50 U.S.C. §§ 1806(f)-(h), 1809(a), 1810.

## STATEMENT OF THE CASE

### A. Legal Background

#### 1. The State-Secrets Privilege

As established by *U.S. v. Reynolds*, 345 U.S. 1 (1953), the state-secrets privilege is a common-law evidentiary privilege that the Court formulated by exercising its "power to determine the procedural rules of evidence." *General Dynamics Corp. v. U.S.*, 563 U.S. 478, 485 (2011). Where the government sustains its burden of showing the evidence is secret and that the other requirements privilege are met, "[t]he privileged information is excluded and the trial goes on without it." *Id*.

The Court is currently considering the relationship of public facts to the state-secrets privilege in *U.S. v. Abu Zubaydah*, No. 20-827—issues that overlap those presented in petitioners' case. The Electronic Frontier Foundation's amicus brief in *Abu Zubaydah* (filed Aug. 20, 2021) presents a more extensive discussion of the state-secrets privilege.

*Reynolds* sets out a balancing approach for courts to use in determining whether the state-secrets privilege applies. 345 U.S. at 7-11. Courts must

independently balance the strength of the government's showing of "reasonable danger" from the production of the evidence against the requesting party's need for the evidence. *Id*. The greater the necessity of the evidence to the party seeking it, the more the government needs to substantiate its claim of potential harm. *Id*.

In cases "[w]here there is a strong showing of necessity [by the requesting party], the claim of privilege should not be lightly accepted," and the court may probe further "in satisfying itself that the occasion for invoking the privilege is appropriate." *Reynolds*, 345 U.S. at 11. While not "automatically require[d]," in such cases the court may review the evidence *in camera* to assess whether it is privileged and, if so, to determine the scope of the privilege. *Id*. at 10.

"Judicial control over the evidence in a case cannot be abdicated to the caprice of executive officers." *Reynolds*, 345 U.S. at 9-10. "[A] complete abandonment of judicial control would lead to intolerable abuses." *Id*. at 8.

As the Court explained in *General Dynamics*, the state-secrets privilege only excludes evidence. It is distinct from the special rule that government-contract disputes are nonjusticiable if "too many of the relevant facts remain obscured by the state-secrets privilege to enable a reliable judgment." *General Dynamics*, 563 U.S. at 492. The government-contract nonjusticiability rule springs not from the Court's "power to determine the procedural rules of evidence, but [its] common-law

authority to fashion contractual remedies in Government-contracting disputes." *Id*. at 485-86 (citing two spy-contract cases: *Totten v. U.S.*, 92 U.S. 105 (1876); *Tenet v. Doe*, 544 U.S. 1 (2005)).

Because this case is not a government-contract dispute, the nonjusticiability rule does not apply. Yet, notwithstanding this Court's guidance in *General Dynamics*, the lower courts have turned the state-secrets privilege into an expansive and ill-defined rule of nonjusticiability. *See*, *e.g.*, *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070 (9th Cir. 2010) (en banc). Rather than respecting the different origins and functions of the state-secrets evidentiary privilege and the government-contract nonjusticiability rule, the lower courts have merged the two doctrines. *Id*. at 1089; *El-Masri v. U.S.*, 479 F.3d 296, 306 (4th Cir. 2007). The consequence is the abdication of the Judiciary's duty to adjudicate challenges to Executive conduct whenever the claims touch upon issues of national security.

### 2. FISA Overview

The Foreign Intelligence Surveillance Act (FISA; 50 U.S.C. §§ 1801-1818) and the Wiretap Act (18 U.S.C. §§ 2510-2523) together form a comprehensive system regulating electronic surveillance within the United States. The two statutes permit electronic surveillance in designated circumstances pursuant to judicial authorization and prohibit surveillance they do not affirmatively authorize.

Congress enacted FISA in the wake of scandalous revelations of widespread unconstitutional surveillance of Americans conducted in the name of national security. To ensure the Executive could not evade the limits Congress imposed, Congress expressly provided that FISA, the Wiretap Act, and the Stored Communications Act (SCA) are "the exclusive means" by which electronic surveillance and the interception of domestic wire, oral, and electronic communications may be conducted. 18 U.S.C. § 2511(2)(f); 50 U.S.C. § 1812(a).

Given these past Executive abuses, Congress's mandate of statutory exclusivity would become a reality only if Congress also created mechanisms for judicial enforcement of the comprehensive procedural and substantive limitations it imposed on electronic surveillance. Accordingly, FISA subjects electronic surveillance to judicial review both *before* and *after* it occurs.

FISA created the Foreign Intelligence Surveillance Court (FISC) and requires (with limited exceptions) that the government obtain an order from the FISC *before* conducting domestic surveillance for foreign intelligence purposes. *See* 50 U.S.C. §§ 1804, 1805. The FISC reviews applications for electronic surveillance according to statutory criteria and grants or denies orders authorizing the surveillance. Pre-surveillance judicial review allows the FISC to enforce the substantive limitations FISA imposes on surveillance.

FISA and 18 U.S.C. § 2712 (discussed below) also provide for judicial review of electronic surveillance

*after* it occurs. They do so by creating criminal and civil liability for unlawful electronic surveillance (18 U.S.C. § 2712; 50 U.S.C. §§ 1809, 1810) and by providing for the exclusion of unlawfully-obtained surveillance evidence (50 U.S.C. § 1806(e)). They also do so through section 1806(f)'s requirement that courts grant discovery of state-secrets evidence in cases of unlawful surveillance.[1]

Section 1806(f) provides the practical means by which the civil liability created to protect the exclusivity of FISA and the Wiretap Act and enforce substantive limitations on surveillance can be litigated without endangering national security. Thus, both the civil remedies and section 1806(f)'s discovery procedures are essential elements of Congress's comprehensive statutory scheme.

FISA's criminal and civil remedies in sections 1809 and 1810 apply regardless of whether the surveillance was conducted for a foreign-intelligence purpose. Sections 1809 and 1810 apply to all surveillance within FISA's broad definition of "electronic surveillance" (50 U.S.C. § 1801(f)). That definition encompasses not only FISA surveillance but also electronic surveillance unrelated to foreign intelligence investigations, electronic surveillance that could never be authorized under FISA, and surveillance prohibited by the Wiretap Act or the SCA. Thus, unlawful surveillance may

[1] The Electronic Frontier Foundation's amicus brief in *FBI v. Fazaga*, No. 20-828 (filed Sept. 28, 2021), presents a more extensive discussion of sections 1806(f) and 2712(b)(4), and their displacement of the state-secrets privilege.

simultaneously violate sections 1809 and 1810, the Wiretap Act, and the Constitution, as Congress recognized. H.R. Rep. No. 95-1283, pt. I, at 97 (1978).

### 3. Section 1806

Congress recognized that in civil actions challenging unlawful electronic surveillance, the evidence may include secret information. In section 1806(f), Congress established a procedure enabling those actions to go forward to a decision on the merits while protecting the secrecy of the information. Rather than excluding secret evidence, as might occur under the state-secrets privilege, Congress instead displaced the state-secrets privilege and directed courts to determine the discoverability of the secret evidence by examining it *in camera* and *ex parte* to decide whether the surveillance was illegal. Only if the surveillance was illegal does the court grant the discovery request.

If the court grants discovery, then the evidence is in the case for all purposes, including standing and the merits, just as is true whenever evidence is produced in response to a discovery request. The court can use its power to craft protective orders under Federal Rule of Civil Procedure 26 to protect secret evidence from public disclosure while providing the plaintiff an opportunity to litigate its case.

The case then proceeds forward using the evidence produced pursuant to section 1806(f) along with any other evidence the parties develop. The court's initial determination when deciding a discovery motion

under section 1806(f) that the surveillance was illegal is a preliminary and interlocutory one, just as any factual determination made in the course of litigating a discovery issue is an interlocutory one not binding on the factfinder at trial. *See* Fed. R. Civ. P. 54(b).

In *Fazaga*, the Court is considering the role of section 1806(f) in civil litigation and its displacement of the state-secrets privilege.

The following examination of section 1806's text explains its operation in civil actions challenging unlawful surveillance and confirms that the statute displaces the state-secrets privilege in this case.

**Sections 1806(a)-1806(e):** Sections 1806(a)-1806(e) address the government's use of electronic-surveillance evidence. Section 1806(a) requires minimization and limits the use of FISA-acquired information. Section 1806(b) requires Attorney General approval of use of FISA-acquired information in criminal proceedings. Sections 1806(c) and 1806(d) require notice if the federal or state governments seek to use electronic-surveillance evidence in a legal proceeding. Section 1806(e) addresses grounds for motions to suppress electronic-surveillance evidence.

**Section 1806(f):** The first sentence of section 1806(f) begins with three "whenever" clauses that lay out three different circumstances in which section 1806(f) applies.

Clause one addresses situations, described in sections 1806(c)-(d), in which the government is seeking

to introduce electronic-surveillance evidence; clause two addresses motions where a party is seeking to suppress such evidence under section 1806(e): "Whenever a court or other authority is notified pursuant to subsection (c) or (d), or whenever a motion is made pursuant to subsection (e), . . . ." § 1806(f).

Clause three, however, addresses circumstances in which a person subjected to electronic surveillance is seeking to discover evidence relating to the surveillance: "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. . . ." § 1806(f). It is clause three that applies when a private plaintiff seeks discovery of surveillance-related evidence.

"[*A*]*ny* motion or request . . . pursuant to any other statute or rule . . . to discover or obtain" encompasses any discovery request of whatever kind, including civil discovery requests by private parties. § 1806(f) (emphasis added); *Ali v. Federal Bureau of Prisons*, 552 U.S. 214, 218-28 (2008). "Read naturally, the word 'any' has an expansive meaning, that is, 'one or some indiscriminately of whatever kind.'" *U.S. v. Gonzales*, 520 U.S. 1, 5 (1997). "Congress did not add any language limiting the breadth of that word," *id*., and so it must be read to encompass all "motion[s] or request[s]" to

"discover or obtain applications or orders or other materials relating to electronic surveillance," § 1806(f).

Clause three thus includes any discovery requests by a civil plaintiff suing the government and seeking materials relating to electronic surveillance. "A decision of illegality [of government surveillance] may not always arise in the context of suppression; rather it may, for example, arise incident to a discovery motion in a civil trial." H.R. Rep. No. 95-1283, pt. I, at 93. The House-Senate Conference Committee's explanation of the statutory text negotiated by the two chambers confirms that section 1806(f) applies to civil cases: "The conferees agree that an in camera and ex parte proceeding is appropriate for determining the lawfulness of electronic surveillance in both criminal and civil cases." H.R. Rep. No. 95-1720, at 32.

When a plaintiff makes a discovery request to obtain materials relating to electronic surveillance, section 1806(f) puts the government to a choice. It can provide the requested materials pursuant to its discovery obligations under the rules of civil procedure. Or, if "disclosure [of the materials] . . . would harm the national security" the government can invoke section 1806(f)'s *ex parte*, *in camera* review procedures. Under section 1806(f), there is no additional alternative.

Reviewing the evidence *in camera* and *ex parte*, the district court then "determine[s] whether the surveillance of the aggrieved person was lawfully authorized and conducted." § 1806(f).

**Section 1806(g):** Section 1806(g) says what happens next, after the district court determines the lawfulness of the surveillance. If the surveillance was unlawful, the court "shall . . . grant the motion of the aggrieved person." § 1806(g). This mandatory language leaves the court with no discretion. In the case of a civil discovery motion seeking surveillance-related evidence, granting the discovery motion means that the evidence is available for use in deciding any issue in the case to which it is relevant, including standing and the merits. The district court may impose appropriate security procedures and protective orders, as in any civil litigation.

The government has argued in *Fazaga* that section 1806(f)'s *in camera*, *ex parte* procedures, even if they apply to discovery and evidence admissibility rulings, do not apply when the district court reaches the post-discovery stage of determining the merits of a cause of action alleging unlawful surveillance. If the Court adopts that view, there is nothing inconsistent with that conclusion and the statutory interpretation petitioners set forth here. Because the section 1806(f) determination of the legality of the surveillance process is part of the decision of a discovery motion, it is an interlocutory order like any factual determination made in the course of determining a discovery motion. But those interlocutory factual determinations made in the course of discovery proceedings are not binding on the factfinder at trial. Instead, if the court in the section 1806(f) proceeding determines the surveillance was unlawful, all that happens is the evidence comes

into the case and is equally available for use by all parties at the merits stage, under whatever protective measures the court has imposed. The merits stage then proceeds as it otherwise would.

If instead "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." § 1806(g). So even if the court determines the surveillance was lawful, discovery still occurs in those circumstances where due process requires it.

**Section 1806(h):** Section 1806(h) provides the government with a number of safety valves to protect against the erroneous disclosure or use of national security information. It does so by making a series of the district court's decision points each into final orders immediately appealable under 28 U.S.C. § 1291. "Orders granting motions or requests under subsection (g), decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance shall be final orders. . . ." § 1806(h).

The government's multiple rights to immediate appellate review give strong protections that there will be no erroneous disclosure of surveillance-related materials. *See* H.R. Rep. No. 95-1720, at 32 (1978) (Conf. Rep.).

**Summary:** When a litigant makes a discovery request or motion seeking surveillance-related evidence and the government asserts that disclosure of the evidence would harm national security, section 1806(f) provides, "notwithstanding any other law," that the court "shall" review the evidence *in camera* and *ex parte* and determine whether the surveillance was lawful. If it was unlawful, the court "shall" grant the discovery motion. § 1806(g).

#### 4. Congress Expanded The Use Of Section 1806(f) In The USA PATRIOT Act

In 2001 in the USA PATRIOT Act, Congress reaffirmed and expanded the use of section 1806(f) in civil litigation by adding 18 U.S.C. § 2712. Section 2712 creates a civil cause of action against the United States for violations of the Wiretap Act and the SCA, as well as violations of select provisions of FISA. (It replaced an earlier cause of action against the government under 18 U.S.C. § 2511.)

Section 2712(b)(4) expands section 1806(f)'s scope to include not just evidence relating to "electronic surveillance" as defined in FISA but also evidence relating to interceptions of communications under the Wiretap Act and the acquisition of communications records under the SCA. In lawsuits like this one presenting Wiretap Act or SCA claims, section 2712(b)(4) mandates that, "[n]otwithstanding any other provision of law," section 1806(f)'s procedures are the "exclusive means" for handling "materials governed by" section 1806(f).

The materials governed by section 1806(f) are materials whose "disclosure . . . would harm the national security," i.e., state secrets. § 1806(f).

### 5. 18 U.S.C. § 2712 And 50 U.S.C. § 1806(f) Displace The State-Secrets Privilege

The state-secrets privilege does not apply to this lawsuit because section 1806(f) displaces it. Congress has the power to displace evidentiary privileges by statute. *Usery v. Turner Elkhorn Mining Co.*, 428 U.S. 1, 31 (1976). Congress has also set the standard by which the question of displacement of the state-secrets privilege is judged. Federal Rule of Evidence 501 provides "[t]he common law . . . governs a claim of privilege unless any of the following provides otherwise: . . . a federal statute."

Section 1806(f) meets Rule 501's displacement test: it is a statute that "provides otherwise" for the discovery and use, under special protective procedures, of surveillance-related evidence that the state-secrets privilege might otherwise exclude. Section 1806(f) thereby displaces the common-law state-secrets privilege that would otherwise apply under Rule 501.

The overlap between section 1806(f) and the state-secrets privilege is self-evident. The state-secrets privilege addresses evidence whose public disclosure would harm national security. The subject matter of section 1806(f) is the same: evidence whose "disclosure . . . would harm the national security." § 1806(f).

Further, Congress expressly provided that section 1806(f) applies "notwithstanding any other law," thus confirming its intent to displace the "other law" of the state-secrets privilege. § 1806(f). Section 1806(f) directs courts, rather than excluding evidence whose disclosure would harm national security, to use the evidence to decide the lawfulness of the surveillance and, if the surveillance is unlawful, to grant discovery of the evidence for use in the lawsuit. Thus, it is plainly contrary to the state-secrets privilege's exclusion of such evidence.

Section 1806(f) leaves no room for the state-secrets privilege to operate. Section 1806(f) and the state-secrets privilege are mutually exclusive. Applying the state-secrets privilege to exclude evidence relating to illegal surveillance would mean nullifying section 1806(f).

Section 2712 independently displaces the state-secrets privilege. It is equally explicit in "provid[ing] otherwise" for the admission of evidence that the state-secrets privilege might otherwise exclude. Fed. R. Evid. 501. It, too, applies "[n]otwithstanding any other provision of law," and provides in section 2712 lawsuits that section 1806(f)'s procedures are the "exclusive means" for reviewing materials relating to electronic surveillance whose disclosure would harm national security. 18 U.S.C. § 2712(b)(4).

Even if Rule 501 did not govern, sections 1806(f) and 2712(b)(4) would still displace the state-secrets privilege by their express terms.

Where federal "common-law adjudicatory principles" like the state-secrets privilege are at issue, all that is required is that "'a statutory purpose to the contrary is evident.'" *Astoria Federal Savings & Loan Ass'n v. Solimino*, 501 U.S. 104, 108 (1991). Congress is not required to "state precisely any intention to overcome" the state-secret privilege's application to FISA. *Id.* Section 1806(f)'s statutory purpose of using secret evidence to decide discovery requests seeking materials relating to surveillance and to grant discovery if the surveillance was unlawful is plainly contrary to the state-secrets privilege's purpose of excluding secret evidence. Section 2712(b)(4)'s command to use section 1806(f)'s procedures is equally contrary.

Even if the "speaks directly" test governed instead of Rule 501's "provides otherwise" or *Astoria's* "contrary purpose" standards, it is satisfied here. Section 1806(f) "'speak[s] directly to [the] question' at issue" under the state-secrets privilege: the use of evidence whose disclosure would harm national security. *American Electric Power Co. v. Connecticut*, 564 U.S. 410, 424 (2011). "Congress need not 'affirmatively proscribe' the common-law doctrine at issue." *U.S. v. Texas*, 507 U.S. 529, 534 (1993).

Section 1806(f) speaks directly to the admissibility and use of state-secrets evidence relating to electronic surveillance. It establishes a different standard and a different procedure for determining whether the evidence is discoverable—procedures that the district court "shall" use, that apply "notwithstanding any other law," and that are manifestly incompatible with

the state-secrets privilege. § 1806(f). Section 2712(b)(4) likewise "speaks directly." The textual commands in these two statutes necessarily displace the "other law" of the state-secrets privilege.

Finally, even if the state-secrets privilege is held to have a constitutional basis, Congress still has authority to regulate it by measures such as sections 1806(f) and 2712(b)(4) addressing the use of military secrets in litigation. Congress's war powers "To make Rules for the Government and Regulation of the land and naval Forces," Const., art. I, § 8, cl. 14, extends to "Rules for the Government and Regulation" of intelligence surveillance, including the power to determine when and how surveillance-related materials should be used in litigation. *See Hamdan v. Rumsfeld*, 548 U.S. 557, 593 n.23 (2006) (President "may not disregard limitations that Congress has, in proper exercise of its own war powers, placed on his powers.").

### 6. Standing

"The plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016).

## B. Factual And Procedural Background

### 1. Introduction

Beginning in 2001, our government instituted an unprecedented regime of domestic mass surveillance, seizing and searching the communications and communications records of hundreds of millions of Americans whom the government suspects of nothing.

Three forms of mass surveillance are at issue here.

One form of mass surveillance, called "Upstream," involves the mass interception and suspicionless searching of email and other Internet communications as they pass through key junctions of the Internet "backbone." Privacy and Civil Liberties Oversight Board ("PCLOB"), *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (ER 393-588).[2]

Another form of mass surveillance involves the suspicionless collection of all phone records for all subscribers from major telephone companies. PCLOB, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* (ER 152-389).

The third form is the mass collection of Internet metadata. According to the FISC, the government collected metadata for "all email" "traversing any of the

---

[2] "ER" citations are to the Excerpts of Record in No. 19-16066 (9th Cir.; vols. 1-7 filed Sept. 6, 2019; vol. 8 filed Oct. 15, 2019).

communications facilities" in the program, and over time greatly expanded the range of facilities. ER 616-21, 667, 673. It was a "massive" collection program—"sweeping" and "wholly non-targeted bulk production." ER 666, 673, 707.

When they began in 2001, these three forms of mass surveillance proceeded solely on presidential authorization, with no involvement by the FISC or any other judicial body. ER 192-201, 413-20. Years later, the FISC began issuing orders authorizing the surveillance. *Id*. The FISC never looked back to address the lawfulness of the mass surveillance that the President unilaterally authorized. The FISC's supervision of the surveillance has been marked by government noncompliance and misrepresentations to the FISC, followed by FISC opinions chastising the government and finding its past practices unlawful and/or unauthorized, followed by more government noncompliance and misrepresentations, followed by more chastisement and correction from the FISC, and so on. *See*, *e.g.*, ER 201-09, 594-95, 601-14, 664, 699-700, 715-17, 725-27 & nn. 14-15, 822-24; ECF No. 358-1 at 19-20.[3]

For the past twenty years, the government has sought to avoid any adjudication of the legality of these mass-surveillance programs. Key to the government's evasion of accountability has been its invocation of the state-secrets privilege to obtain dismissals of challenges to these programs.

---

[3] "ECF" citations are to the district court's docket in *Jewel v. NSA*, No. 08-CV-04373-JSW (N.D. Cal.).

Petitioners are ordinary Americans whose communications and communications records were caught up in the government's mass surveillance. They are AT&T and Verizon phone customers whose phone records were collected in bulk by the government and searched. They are AT&T Internet customers whose Internet communications, including metadata, were intercepted, copied, and searched.

### 2. District Court Proceedings

Petitioners filed suit in 2008 challenging Upstream, the phone records program, and the Internet metadata program. They bring claims against the government and official-capacity defendants under the Fourth Amendment, the Wiretap Act, and the SCA. ER 1115-49 (Counts I, IX, XII, XV). Petitioners bring their Fourth Amendment claims individually and as representatives of an injunctive-relief-only class comprising AT&T's customers. ER 1115-17 (Count I).

Petitioners bring claims against the individual-capacity defendants under the Fourth Amendment, FISA, the Wiretap Act, and the SCA. ER 1117-49 (Counts II, VI, VIII, XI, XIV).

The district court had jurisdiction under 18 U.S.C. § 2712 and 28 U.S.C. § 1331.

After the Ninth Circuit reversed the district court's erroneous 2010 dismissal for lack of standing (*Jewel v. NSA*, 673 F.3d 902 (9th Cir. 2011)), the district court held that sections 1806(f) and 2712(b)(4)

displaced the state-secrets privilege. *Jewel v. NSA*, 965 F.Supp.2d 1090, 1103-06 (N.D. Cal. 2013); ER 56-80. It accordingly required the government to respond to petitioners' discovery requests and produce any state-secrets evidence *ex parte* and *in camera* to the Court. ER 36; 5/19/17 RT 49-54, 67-74.[4] Independently, the district court ordered the government to marshal and present all of the classified evidence relevant to petitioners' standing, regardless of whether it fell within petitioners' requests. ER 36; 5/19/17 RT 49-54, 67-74.

The government responded *ex parte* and *in camera* with a 193-page classified declaration from NSA Director Rogers, together with thousands of pages of classified documents. ECF Nos. 388, 389-1, 389-2, 389-3, 411 at 6. None of this evidence was disclosed to petitioners. The district court denied petitioners' motions, pursuant to section 1806(f) and subject to security clearances, for access to the classified materials. ECF Nos. 393, 400, 401, 417-1; ER 34-35. Petitioners also objected that the government had failed to respond to their interrogatories and requests for admission in the form required by the Federal Rules of Civil Procedure and moved to compel proper responses; the district court denied the motion. ECF No. 411; ER 29.

The district court then ordered the government to move for summary judgment on petitioners' standing. ER 31-32. It ordered the government to brief the public and secret evidence relating to petitioners' standing

---

[4] "RT" cites are to the Reporter's Transcript in *Jewel v. NSA*, No. 08-CV-04373-JSW (N.D. Cal.).

and limited petitioners to briefing the public evidence only. ER 32. Petitioners opposed the government's summary judgment motion and cross-moved for an order directing the case to proceed to trial. ECF Nos. 417, 429-3. Pursuant to Federal Rule of Civil Procedure 56(d), they also renewed their discovery objections and their request for access to the classified materials, which the district court again denied. ECF No. 417-1; App. 43a-44a.

### 3. Petitioners' Evidentiary Showing

To show injury-in-fact and traceability, petitioners only need to show that a reasonable factfinder could conclude it is more likely than not that the government has interfered with their communications and communications records. They do not need to prove that the interference violated the Constitution, FISA, the Wiretap Act, or the SCA. Standing "in no way depends on the merits of the plaintiff's contention that particular conduct is illegal." *Warth v. Seldin*, 422 U.S. 490, 500 (1975).

#### (a) Standing Relating To Phone Records Collection Claims

It is undisputed that from 2001 to 2015 the government collected all of the phone records of major telephone companies. The FISC describes the phone records program as the "production by major telephone service providers of call detail records for all domestic,

United States-to-foreign, and foreign-to-United States calls." ER 666; *accord* ER 177, 270.

So the only question for standing is whether petitioners' telephone providers, AT&T and Verizon, were part of the phone records program. AT&T and Verizon are the two largest telephone companies. AT&T and Verizon admitted they provided "non-content" information—i.e., communications records—about their customers' communications to the government pursuant to FISC orders. ER 911, 928.

In 2015, as a settlement of FOIA litigation the government produced to the *New York Times* a NSA document identifying AT&T, Verizon, and Sprint as participants in the phone records collection program. ER 869; ER 896-97; ER 845-46, ¶¶3, 4; ER 849-67; ER 147-48, ¶¶2-3, 5-6; *see* AOB 27-28.[5] Petitioners submitted a declaration from counsel for the *New York Times* verifying receipt of the NSA document from the government. ER 147-48. The government says the document's disclosure was inadvertent, but that does not make the document any less public. ER 148, ¶¶7-9. The document remains available on the *New York Times*' website.[6]

The *New York Times* NSA document alone is sufficient evidence from which a reasonable factfinder

---

[5] "AOB" cites are to Appellants' Opening Brief, No. 19-16066 (Ninth Circuit, filed Oct. 7, 2019). "ARB" cites are to Appellants' Reply Brief, No. 19-16066 (Ninth Circuit, filed Jan. 27, 2020).

[6] https://www.nytimes.com/interactive/2015/08/12/us/nsa-foia-documents.html, at p. 111 (accessed Jan. 9, 2022).

could find it more likely than not that petitioners' phone records were collected by the government. Petitioners also submitted other evidence corroborating AT&T and Verizon's participation in the phone records collection program. AOB 26-36 (reviewing evidence). No doubt the classified evidence produced by the government, if responsive to the district court's production order, contains further evidence verifying the collection of petitioners' phone records. AOB 59-60 (identifying evidence petitioners expect is in the classified evidence).

**(b) Standing Relating To Upstream Internet Interception And Internet Metadata Claims**

Petitioners presented extensive evidence showing their emails, other Internet communications, and Internet metadata were intercepted, copied, and diverted into the restricted-access "SG3 Secure Room" at AT&T's Folsom Street Facility in San Francisco. AOB 39-43, 79-88 (reviewing evidence); ARB 32-38 (same).

In district court, the government conceded that petitioners' evidence was sufficient to show their Internet communications and metadata had been intercepted, copied by "splitters," and the copies diverted into the SG3 Secure Room.

The government admitted petitioners' evidence shows:

> (iii) That online communications traffic crossing 'peering links' located at AT&T's Folsom Street, San Francisco, facility is electronically copied, using optical splitters, and the entire copied stream diverted to a room designated as the SG3 Secure Room, . . . ; (iv) That since 2001 at least one of each Plaintiff's Internet communications has transited the 'peering links' located at Folsom Street, and the copy 'redirected' to the SG3 Secure Room.

ECF No. 421 at 13:2-14.

The undisputed interception, copying, and diversion of petitioners' Internet communications is an injury-in-fact. *See U.S. v. Szymuszkiewicz*, 622 F.3d 701, 705-07 (7th Cir. 2010) (copying and diverting emails violates the Wiretap Act); *Noel v. Hall*, 568 F.3d 743, 749 (9th Cir. 2009) (Wiretap Act interception "occurs 'when the contents of a wire communication are captured or redirected in any way'"); *U.S. v. Councilman*, 418 F.3d 67, 79 (1st Cir. 2005) (en banc) (interception, copying, and diversion of emails violated the Wiretap Act); *U.S. v. Rodriguez*, 968 F.2d 130, 136 (2d Cir. 1992) ("when the contents of a wire communication are captured or redirected in any way, an interception occurs").

Thus, given the government's concession that petitioners' communications were intercepted, copied, and diverted, the question was not, as the Ninth Circuit erroneously believed (App. 2a), whether petitioners had shown an injury-in-fact (standing's first

element); the question was whether that injury more likely than not was fairly traceable to the government's surveillance programs (standing's second element).

Petitioners presented extensive evidence that the interception, copying, and diversion of their communications is fairly traceable to the government.

Petitioners' evidence included government admissions about Upstream's scope and nature and its technical operation. Upstream collects communications as they are in transit on the Internet backbone—high-capacity circuits operated by major Internet providers: "[T]he [NSA] intercepts communications directly from the Internet 'backbone'" using "NSA-designed upstream Internet collection devices [that] acquire transactions as they cross the Internet." ER 521, 436; *see also* ER 404, 432-38, 481.

The interceptions occur at the point where the Internet backbone circuits of different Internet providers connect, "in the flow of communications between communication service providers." ER 432. These connections between communication service providers are called "peering links," and that is exactly where the splitters in the Folsom Street Facility are located. ER 991, ¶48(e); ER 970-71, ¶¶34-36.

AT&T admits it provides communications content to the government pursuant to FISC orders. ER 911.

Petitioner also presented the declaration of the AT&T employee who operated the splitters and was

responsible for transmitting the copied communications of petitioners into the secret SG3 Secure Room. ER 1209-15. The declaration included AT&T documents corroborating his statements. The AT&T documents detail the technical layout of the splitters and their diversion of communications to the SG3 Secure Room, and identify equipment inside the SG3 Secure Room designed to rapidly search enormous volumes of communications. ER 1216-1339.

The employee described the splitters, their placement in the "peering links" interconnecting AT&T's Internet backbone circuits with other Internet providers, and the splitters' copying and diversion of all the communications passing through them into the SG3 Secure Room. ER 1211-15. He described how only AT&T employees cleared by the NSA were permitted in the SG3 Secure Room, contrary to AT&T's policy otherwise allowing employees full access to all areas of the Folsom Street Facility. ER 1212. He described visits he observed by NSA representatives to meet with AT&T employees. ER 1211-12. He described communications he received from his supervisors discussing upcoming NSA visits. *Id*.

AT&T's Managing Director-Asset Protection, a witness adverse to petitioners, affirmed the authenticity of the AT&T documents and affirmed the existence of the splitters, the SG3 Secure Room, and the equipment within the SG3 Secure Room. ER 1196-1205.

Petitioners presented supporting expert declarations from Google's former Director of Operations, from

the Federal Communications Commission's former Senior Advisor for Internet Technology, from a University of Pennsylvania Professor of Computer Science, and from the Federal Trade Commission's former Chief Technologist. ER 1033-70; ER 960-98. The government put in no expert evidence.

Petitioners also presented a government document published by the *Guardian* newspaper supporting petitioners' standing on their phone-records claims, their Internet content-interception claims, and their Internet metadata claims. ECF No. 147; ER 87. Petitioners submitted additional evidence as well of the Internet metadata collection program, which existed from 2001 to 2011, and AT&T's participation in it. AOB 55-58 (reviewing evidence).

From petitioners' evidence, a reasonable factfinder could find it more likely than not that the undisputed interception and copying of petitioners' Internet communications and metadata is fairly traceable to the government. AOB 36-58, 79-88 (reviewing evidence). Petitioners expect the classified evidence produced by the government contains further evidence showing the government's involvement. AOB 59-60 (identifying evidence petitioners expect is in the classified evidence).

#### 4. The District Court's Orders

The district court granted judgment for all defendants. ER 1. The district court issued two orders, a public order and in addition a classified order which petitioners have never seen. App. 5a-44a, 45a. The

public order dismissed the action on state-secrets privilege grounds. App. 14a, 31a-34a, 41a-43a.

The district court held that the state-secrets privilege made petitioners' claims nonjusticiable. App. 14a, 31a-34a, 41a-43a (At 32a: "[T]he Court has determined that it cannot render a judgment either as to the merits or as to any defense on the issue of standing." At 33a: "The Court cannot issue any determinative finding on the issue of whether or not Plaintiffs have standing. . . ."), 42a (granting the government summary judgment because "it cannot rule whether or not Plaintiffs have standing to proceed and that the well-founded assertion of [the state-secrets] privilege mandates dismissal"). It rejected petitioners' argument that section 1806(f) displaces the state-secrets privilege but ignored their argument that section 2712(b)(4) also displaces the state-secrets privilege. App. 39a-41a.

The district court's classified order adjudicates whether the public and classified evidence establishes petitioners' standing: "[T]he Court must review and adjudicate the effect of the classified evidence regarding Plaintiffs' standing to sue. That review and adjudication is contained in the Court's Classified Order filed herewith." App. 23a. Petitioners do not know whether the district court found they have standing.

The district court excluded the *New York Times* NSA document on the ground that it was a state secret, notwithstanding its ongoing publication by the *Times* and its disclosure by the government to the *Times*. App. 28a-29a. The district court also excluded

on state-secrets grounds the *Guardian* NSA document, as well as on authentication grounds. App. 29a-30a.

The district court discounted much of the declaration of the AT&T employee who operated the splitters, transmitted the copied communications and metadata to the SG3 Secure Room, observed NSA representatives coming to meeting with his co-workers, was notified of upcoming meetings with the NSA, and used the AT&T documents in the course of his employment. App. 24a-25a; *see* AOB 49-53. The district court excluded the AT&T documents as hearsay. App. 25a; *see* AOB 46-49. The district court excluded the declaration of AT&T's Managing Director-Asset Protection confirming the authenticity of the AT&T documents and the accuracy of the descriptions of the Folsom Street Facility's equipment in the AT&T documents and in the employee's declaration. App. 25a; *see* AOB 45-46. The district court excluded all of petitioners' expert evidence. App. 26a-27a; *see* AOB 53-54.

### 5. The Ninth Circuit's Decision

In a three-page unpublished opinion remarkably lacking in analysis, the Ninth Circuit summarily affirmed the judgment on the ground that petitioners had failed to establish their standing, even if all the public evidence excluded by the district court was considered. App. 3a. It also held that the district court did not abuse its discretion in excluding public evidence on various grounds and in denying petitioners access to the classified evidence. App. 3a. It did not decide

whether the district court properly applied section 1806(f) or whether it properly dismissed the case under the state-secrets privilege. App. 4a.

The panel did not present any examination or analysis of any item of evidence in petitioners' 1000-page evidentiary record supporting their standing. The panel did not present any analysis of the basis for admissibility and supporting legal authorities that petitioners presented for each item of excluded evidence, or offer any reasoning supporting its unexplained conclusion that there was no error in any of the district court's evidentiary exclusions.

The panel did not review or adjudicate the district court's classified order, which analyzed the classified evidence. It ignored the classified order completely.

The panel did not examine any of the classified evidence. It did not examine the classified Rogers declaration responding to petitioners' discovery requests or any of the classified documents produced in discovery. It reasoned that it was not required to do so because petitioners, who never had access to the classified evidence or the classified order, had not identified specific classified evidence supporting their standing. "Their argument that, pursuant to the procedures set forth in 50 U.S.C. § 1806(f), they may use classified evidence to establish their standing ignores the fact that it is their 'burden to prove their standing by pointing to specific facts,' which they have failed to do here." App. 3a.

In fact, even though petitioners were without access to the classified evidence, they presented to the

Ninth Circuit a long list of the evidence supporting their standing that they expected was present in the classified evidence. AOB 59-60. And the panel's reasoning does not explain why it refused to review the district court's classified order.

## REASONS FOR GRANTING CERTIORARI

### I. The Lower Courts' State-Secrets Jurisprudence And Section 1806(f)/Section 2712(b)(4) Jurisprudence Require The Court's Intervention, And This Case Is An Appropriate Vehicle For Doing So

As the Court is aware from its consideration of the pending cases of *U.S. v. Abu Zubaydah*, No. 20-827, and *FBI v. Fazaga*, No. 20-828, the lower courts have deviated substantially from the Court's state-secrets teachings. They have transformed state secrets from an evidentiary privilege limited to excluding evidence into a rule of nonjusticiability permitting dismissal of an entire action. And they have refused to recognize the limits Congress has placed on the state-secrets doctrine's operation in section 2712(b)(4) and section 1806(f).

Nevertheless, it appears likely from the course of proceedings to date that the Court's decisions in *Abu Zubaydah* and *Fazaga* will leave unresolved many important questions regarding the state-secrets privilege and section 1806(f) that were within the questions presented in those two cases. And it is certain that the

Court's decisions will not reach section 2712(b)(4) and its interaction with the state-secrets privilege, despite section 2712(b)(4)'s close relationship with section 1806(f).

Nor will the Court's decisions in *Abu Zubaydah* and *Fazaga* address the unique circumstances of secret mass surveillance that are present in this case. Mass surveillance "'alter[s] the relationship between citizen and government in a way that is inimical to democratic society,'" *U.S. v. Jones*, 132 S.Ct. 945, 956 (2012) (Sotomayor, J., concurring; alteration added), giving the government the power to peer into its citizens' private communications at any moment. The effect of the lower courts' rulings is that no-one may challenge mass surveillance unless the government acknowledges that the challenger has been subject to surveillance. That sweeping, and troubling, bar to judicial review of government actions threatening fundamental liberties is worthy of the Court's attention.

Granting this petition would allow the Court to address all of these issues, and to do so on a much more complete record than *Abu Zubaydah* and *Fazaga* present.

*Abu Zubaydah* is a discovery-only proceeding brought by a foreign national seeking evidence for use in a foreign proceeding. It does not present the question of how the state-secrets privilege applies in an action seeking relief on the merits of a claim and does not present claims arising under United States law, as

does this case. These factors may well limit the scope of the Court's holding.

Like *Abu Zubaydah*, this case presents the question of whether the state-secrets privilege extends to public evidence. It does so, however, on a much more extensive and clearer record. Here, because the evidence excluded are documents published by the *New York Times* and the *Guardian*, there is no doubt as to the scope of what is claimed to be public and there is no doubt that the documents actually are public. Moreover, unlike *Abu Zubaydah*, petitioners seek the evidence for use on the merits to vindicate their constitutional and statutory rights as Americans.

*Fazaga* presents both state-secrets and section 1806(f) issues. But it arose at the threshold of the lawsuit, before any party sought discovery and without any determination that section 1806(f) applied and without any use of section 1806(f)'s procedures. It also lacks any section 2712(b)(4) issues. Because of *Fazaga's* preliminary stage, the Court's decision may well leave unresolved many of the state-secrets and section 1806(f) issues potentially present in government-surveillance cases, and actually present in this case. And it will not resolve any question involving closely-related section 2712(b)(4). In addition, *Fazaga* also is an individually-targeted surveillance case, not a mass surveillance case like this one.

In petitioners' lawsuit, by contrast, the district court applied the state-secrets privilege, found the very subject matter of the litigation was not a state secret,

found that section 1806(f) and section 2712(b)(4) displaced the state-secrets privilege, ordered the government to produce secret evidence *ex parte* and *in camera*, and used the secret evidence to decide, in secret, whether or not petitioners have standing. It also, however, excluded under the state-secrets privilege public evidence—including a document the government gave to the *New York Times* and that the *Times* published—and then dismissed the action under the state-secrets privilege as nonjusticiable.

Petitioners' lawsuit thus permits the Court to review a case in which the district court actually applied sections 1806(f) and 2712(b)(4) to compel the *ex parte*, *in camera* production of evidence, and then used the secret evidence to decide petitioners' standing. This allows the Court to examine the operation in practice of the *ex parte*, *in camera* procedures of sections 1806(f) and 2712(b)(4), rather than being forced to guess how those procedures might play out in the course of litigation.

The same reasons that impelled the Court to grant certiorari in *Abu Zubaydah* and *Fazaga* equally support certiorari here. The issues surrounding whether and how unlawful-surveillance claims may be litigated in light of the state-secrets privilege, section 2712(b)(4), and section 1806(f) are equally vital and important whether the petitioner is the government or ordinary Americans seeking to confine the government's surveillance of them within constitutional and statutory limits. Just as it is important for the government to protect secrets, it is equally important that

Americans be afforded the opportunity to protect from government overreach their First and Fourth Amendment rights, as well as the statutory rights Congress has created.

This petition is an appropriate vehicle for addressing these issues, and the likelihood that substantial and significant questions regarding the operation of the state-secrets privilege, section 2712(b)(4), and section 1806(f) will remain unresolved after the decisions in *Abu Zubaydah* and *Fazaga* makes the case for review all the more compelling.

## II. The Issues Presented Here Are Of Exceptional Importance

### A. The Constitutional Design Presumes That The Fundamental Rights Of Americans Will Be Judicially Enforceable Against Government Overreach

At issue here are "extensive surveillance programs that carry profound implications for Americans' privacy and their rights to speak and associate freely." *American Civil Liberties Union v. U.S.*, 142 S.Ct. 22, 23 (2021) (Gorsuch, J., dissenting from denial of cert., joined by Sotomayor, J.). These fundamental constitutional and statutory rights are meaningless if there is no way to enforce them against government overreach.

Congress recognized this. Congress created substantive remedies against unlawful surveillance. Congress also created the procedures for litigating constitutional and statutory challenges to surveillance

in section 2712(b)(4) and section 1806(f). These procedures provide for discovery of secret evidence for use, under secure procedures, in surveillance challenges.

The courts below, and others, have refused to use these procedures to adjudicate constitutional and statutory challenges to surveillance. *See Wikimedia Found. v. NSA*, 14 F.4th 276, 301 (4th Cir. 2021). Throughout its history, the Court has recognized the need for judicial enforcement of the constitutional and statutory rights of the People. This case is no different. When the lower courts refuse to adjudicate these rights, the Court's intervention is called for.

That the Ninth Circuit's fundamentally flawed decision is unpublished should not insulate it from review. From the government's point of view, the district court and Ninth Circuit rulings are a powerful and far-reaching victory. The decisions confirm the government's position that its domestic mass surveillance practices—no matter how unlawful, unconstitutional, unauthorized by the FISC, or in defiance of Congress' statutory commands—are beyond judicial challenge. They confirm the government's position that anything short of an official acknowledgment that the plaintiff was surveilled is insufficient to establish standing, and that by withholding acknowledgment the government can prevent any challenge. They confirm the government's position that the state-secrets privilege is an absolute bar to judicial relief no matter the magnitude of the Executive's violations of the People's rights. They confirm the government's position that the substantive and procedural civil remedies against

unlawful surveillance that Congress granted to Americans in FISA and section 2712 are illusory. They confirm the government's position that the President has the unilateral power to secretly conduct mass surveillance of the communications of virtually all Americans without any court order or congressional approval, as occurred for years with each of these programs, and that the courts are powerless to intervene.

The judicial rulings in the lower courts also are in conflict. The Second Circuit has already adjudicated that the phone records collection program was unlawful, yet the district court here held that the program was too secret to litigate. *ACLU v. Clapper*, 785 F.3d 787, 821 (2d Cir. 2015).

Because of the importance of standing doctrine, the Court has taken an active role in supervising its development and regularly grants certiorari to correct misapplications of it in novel situations. *See*, *e.g.*, *TransUnion LLC v. Ramirez*, 141 S.Ct. 2190 (2021). Granting certiorari here will protect the individual freedoms and liberties of millions of Americans from being denied a judicial forum by the Ninth Circuit's misapplication of standing doctrine to mass surveillance cases.

### B. FISC Review Is No Substitute For An Article III Adjudication Of The Legality Of The Government's Surveillance Programs

The FISC, although it is staffed by Article III judges, does not conduct Article III adjudications. It does not adjudicate cases or controversies between adverse parties. "Article III of the Constitution affords federal courts the power to resolve only 'actual controversies arising between adverse litigants.'" *Whole Woman's Health v. Jackson*, 142 S.Ct. 522, 532 (2021).

And so FISC rulings on surveillance applications are no more conclusive of the legality of the surveillance than an Article I magistrate's ruling on a search warrant application—which is to say not at all conclusive.

They are even less so in the case of the government's applications for mass surveillance like the surveillance at issue here. Unlike traditional search warrants and "traditional" FISA orders, the FISC mass-surveillance orders do not require any degree of individualized suspicion or probable cause for the individuals whose communications are intercepted and whose communication records are collected. *See* 50 U.S.C. § 1861 (phone records orders under FISA section 215); 50 U.S.C. § 1881a (Upstream orders under FISA section 702).

For Upstream orders, the government does not identify the individuals whose communications it intercepts and searches, much less establish probable

cause for surveilling them. Instead, all the FISC hears about and approves are the government's descriptions of procedures that it will later use to intercept en masse and scan communications passing through key Internet junctions–descriptions that are not always accurate and procedures that are not always complied with, *see* Statement of the Case, section B(1). The phone records and Internet metadata collection orders similarly are only approvals of generic collection and searching procedures, divorced from any identification of individuals subjected to them or any showing of individualized suspicion.

That is hardly what the Founders had in mind. "[T]he Founders did not fight a revolution to gain the right to government agency protocols." *Riley v. California*, 573 U.S. 373, 398 (2014). Non-adversarial FISC review of the government's procedures for conducting surveillance is no substitute for judicial review and true Article III adjudication.

## III. Review Is Warranted For The Court To Establish The Court Of Appeals' Duty To Review Classified Dispositive Orders When They Are On Appeal

Classified orders by federal district courts or courts of appeals are an infrequent but regular practice. Yet no rule or statute speaks to them, and this Court has never addressed when a district court is justified in issuing a classified *dispositive* order or the

obligation of a court of appeals to review a classified order when it is appealed.

Here, the district court's classified dispositive order sets forth its ruling on whether plaintiffs have standing. The classified order also contains the district court's evaluation of the evidence, both public and classified, supporting petitioners' standing. Petitioners appealed the classified order, and appealed the district court's denial of access to the classified evidence on which the order was based.

The Ninth Circuit, however, did not adjudicate the district court's classified ruling on petitioners' standing. *Cf. U.S. v. Muhtorov*, No. 18-1366, 2021 WL 5817486, at *13 (10th Cir. Dec. 8, 2021) (court of appeals performed "careful and independent review of the classified record" to determine legality of FISA surveillance).

The Ninth Circuit also did not review any of the classified evidence. It took the position that it had no duty to review the classified evidence since petitioners had not pointed to specific classified evidence supporting their standing—an impossible and clearly erroneous demand by the Ninth Circuit, since the district court had denied petitioners access to both the classified evidence and the classified order. App. 3a. Nonetheless, petitioners did present an extensive list of specific evidence they expected was present in the classified evidence if the government had been forthcoming in responding to petitioners' discovery requests, and requested that the Ninth Circuit review the classified evidence. AOB at 59-60.

The Court should grant certiorari to establish the duty of a court of appeals, when presented on appeal with a classified dispositive order the appellant has never seen but forming part of the basis of the judgment, to review the classified order.

## IV. In The Alternative, The Court Should Hold The Petition Until The Court's Decisions In *Abu Zubaydah* And *Fazaga*, And Then Grant, Vacate, And Remand

As explained above, the questions presented in this petition are closely intertwined with the state-secrets privilege and FISA interpretation issues pending before the Court in *Abu Zubaydah* and *Fazaga*.

Petitioners have filed this petition before the Court's decisions in those two cases, and do not know how the Court will rule. Nevertheless, there is a strong likelihood that the Court's rulings in those cases will implicate the judgment below in this case. If that turns out to be the case, petitioners respectfully request in the alternative that the Court grant their petition, vacate the judgment, and remand for further proceedings consistent with its decisions in those two cases and with specific directions that the Ninth Circuit adjudicate the district court's classified opinion.

For that reason, also, petitioners respectfully request that the Court hold this petition until its decisions in *Abu Zubaydah* and *Fazaga*.

## CONCLUSION

The petition for a writ of certiorari should be granted.

January 2022

Respectfully submitted,

RICHARD R. WIEBE
*Counsel of Record*
LAW OFFICE OF
RICHARD R. WIEBE

THOMAS E. MOORE III
HAYNES AND BOONE, LLP

CINDY A. COHN
DAVID GREENE
LEE TIEN
KURT OPSAHL
ANDREW CROCKER
AARON MACKEY
ELECTRONIC FRONTIER
FOUNDATION

RACHAEL E. MENY
BENJAMIN W. BERKOWITZ
KEKER, VAN NEST &
PETERS LLP

ARAM ANTARAMIAN
LAW OFFICE OF
ARAM ANTARAMIAN

*Counsel for Petitioners*