No. 13-

IN THE

Supreme Court of the United States

IN RE ELECTRONIC PRIVACY INFORMATION CENTER,

Petitioner

On Petition for a Writ of Mandamus and Prohibition, or a Writ of Certiorari, to the Foreign Intelligence Surveillance Court

PETITION FOR A WRIT OF MANDAMUS AND PROHIBITION, OR A WRIT OF CERTIORARI

MARC ROTENBERG
Counsel of Record
ALAN BUTLER
DAVID JACOBS
DAVID BRODY
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

July 8, 2013

QUESTIONS PRESENTED

Congress enacted the Foreign Intelligence Surveillance Act to authorize and regulate certain governmental electronic surveillance of communications for foreign intelligence purposes. In the Act, Congress authorized judges of the Foreign Intelligence Surveillance Court to approve electronic surveillance for foreign intelligence purposes.

In the Order below, the Foreign Intelligence Surveillance Court compelled Verizon Business Network Services to produce to the National Security Agency, on an ongoing basis, all of the call detail records of Verizon customers. Petitioner, a non-profit organization engaged in legal work and advocacy, is a Verizon customer.

The questions presented are:

1. Whether the Foreign Intelligence Surveillance Court exceeded its narrow statutory authority to authorize foreign intelligence surveillance, under 50 U.S.C. § 1861, when it ordered Verizon to disclose records to the National Security Agency for all telephone communications "wholly within the United States, including local telephone calls."
2. Whether Petitioner is entitled to relief pursuant to 28 U.S.C. § 1651(a) to vacate the order of the Foreign Intelligence Surveillance Court, or other relief as this Court deems appropriate.

PARTIES TO THE PROCEEDINGS

The following were parties to the proceedings in the Foreign Intelligence Surveillance Court ("FISC"):

1. Federal Bureau of Investigation ("FBI") filed the application with the FISC for a production order.

The following are parties to this proceeding in the United States Supreme Court:

1. Electronic Privacy Information Center ("EPIC") is the petitioner. EPIC was not a party to the FISC proceedings.
2. The Honorable Roger Vinson, FISC, is the judge to whom mandamus is sought.

TABLE OF CONTENTS

TABLE OF CONTENTS - Continued

TABLE OF AUTHORITIES

CASES

CONSTITUTIONAL PROVISIONS

STATUTES

RULE

LEGISLATIVE MATERIALS

OTHER AUTHORITIES

IN THE

Supreme Court of the United States

IN RE ELECTRONIC PRIVACY INFORMATION CENTER,

Petitioner

On Petition for a Writ of Mandamus and Prohibition, or a Writ of Certiorari, to the Foreign Intelligence Surveillance Court

PETITION FOR A WRIT OF MANDAMUS AND PROHIBITION, OR A WRIT OF CERTIORARI

The Electronic Privacy Information Center ("EPIC") respectfully petitions for a writ of mandamus and prohibition to vacate the order of the Honorable Roger Vinson of the Foreign Intelligence Surveillance Court and prohibit such future orders, or, in the alternative, for a writ of certiorari to review the judgment of the Foreign Intelligence Surveillance Court.

OPINION BELOW

The order of the Foreign Intelligence Surveillance Court is not reported, but is reproduced at Pet. App. 1a-3a.

JURISDICTION

The Foreign Intelligence Surveillance Court entered the Verizon Order on April 25, 2013. This Court's jurisdiction rests on 28 U.S.C. § 1651 and 50 U.S.C. §§ 1803, 1861(f).

STATUTE INVOLVED

The Foreign Intelligence Surveillance Act authorizes certain governmental surveillance of communications for foreign intelligence purposes. 50 U.S.C. §§ 1801 *et. seq*. (2012). Section 1861 allows the Federal Bureau of Investigation ("FBI") to apply to the Foreign Intelligence Surveillance Court ("FISC") for an order to compel production of "tangible things . . . for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1861(a)(1) ("Access to certain business records for foreign intelligence and international terrorism investigations."). The application must include a statement of facts showing "that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation," 50 U.S.C. § 1861(b)(2)(A), and an enumeration of the minimization guidelines adopted by the Attorney General. 50 U.S.C. § 1861(b)(2)(B). If the application meets these statutory requirements, the FISC "shall enter an ex parte order as requested, or as modified, approving the release of tangible things." 50 U.S.C. § 1861(c)(1).

INTRODUCTION

EPIC seeks a writ of mandamus to review the order of Judge Roger Vinson, United States Foreign Intelligence Surveillance Court ("FISC") requiring Verizon Business Network Services ("Verizon") to produce to the National Security Agency ("NSA") call detail records, or "telephony metadata," for all calls wholly within the United States. Mandamus relief is warranted because the FISC exceeded its statutory jurisdiction when it ordered production of millions of domestic telephone records that cannot plausibly be relevant to an authorized investigation. EPIC is a Verizon customer subject to the order. Because of the structure of the Foreign Intelligence Surveillance Act ("FISA"), no other court may grant the relief that EPIC seeks.

On April 25, 2013, the FISC compelled the ongoing disclosure of all call detail records in the possession of a U.S. telecommunications firm for analysis by the National Security Agency. The FISC exceeded its statutory authority when it issued this order. To compel production of "tangible things," the FISA requires the items sought be "relevant" to an authorized investigation. 50 U.S.C. § 1861(b)(2)(A). It is simply not possible that every phone record in the possession of a telecommunications firm could be relevant to an authorized investigation. Such an interpretation of Section 1861 would render meaningless the qualifying phrases contained in the provision and eviscerate the purpose of the Act.

The Verizon Order approved by the FISC implicates the privacy interests of all Verizon customers, including petitioner EPIC, a non-profit organization that engages in protected attorney-

client communications as it pursues litigation to safeguard privacy. However, the FISA does not allow Verizon customers, including, EPIC to challenge the order or seek review of the order before the FISC or Foreign Intelligence Surveillance Court of Review ("Court of Review"). *See* 50 U.S.C. § 1861(f); *id.* §§ 1803(a)-(b); Foreign Intelligence Surveillance Ct. R. 33. Consequently, EPIC can only obtain relief with a writ of mandamus from this Court. Mandamus is an extraordinary remedy, but the Verizon Order carries extraordinary ramifications.

The records acquired by the NSA under this Order detail the daily activities, interactions, personal and business relationships, religious and political affiliations, and other intimate details of millions of Americans. "Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse." *United States v. Jones,* 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring). As Justice Breyer has recently noted, "the Government has the capacity to conduct electronic surveillance of the kind at issue." *Clapper v. Amnesty Int'l, USA*, 133 S.Ct. 1138, 1158-59 (2013) (citing, *inter alia*, Priest & Arkin, *A Hidden World, Growing Beyond Control*, Wash. Post, July 19, 2010, at A1 (reporting that the NSA collects 1.7 billion e-mails, telephone calls and other types of communications daily)). And because the NSA sweeps up judicial and Congressional communications, it inappropriately arrogates exceptional power to the Executive Branch.

STATEMENT OF THE CASE

I. The Foreign Intelligence Surveillance Act

Congress passed the Foreign Intelligence Surveillance Act ("FISA") in 1978 to prevent the indiscriminate and invasive domestic surveillance of Americans by government intelligence agencies. *See* S. Rep. No. 95-604(I) at 7 (1977), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3908 ("This legislation is in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused."); 1 David S. Kris & J. Douglas Wilson, *National Security Investigations & Prosecutions* §§ 2.2-2.6, 3.4 (2d. ed. 2012) (discussing a "history of abuse" within the Intelligence Community) (hereinafter "Kris & Wilson").[1] The FISA required the Government to limit surveillance to specific, targeted investigations of *foreign* agents and *foreign* powers, and it created the *Foreign* Intelligence Surveillance Court ("FISC") to oversee and authorize such surveillance. As Justice Alito recently stated for the Court in *Clapper*:

---

[1] "A modern reader may reasonably ask what motivated the abuses. . . . A review of the historical record suggests that [the Intelligence Community's] excesses were motivated in substantial part by fear." Kris & Wilson § 2.5. The need for a statute and a court to oversee national security surveillance was anticipated several years before enactment of the FISA and the establishment of the FISC. *See* Report of the Chairman – Samuel Alito, *Conference on the Boundaries of Privacy in American Society*, Woodrow Wilson Sch. of Pub. & Int'l Affairs, Princeton Univ. at 5 (Jan. 4, 1972).

> Congress enacted the Foreign Intelligence Surveillance Act (FISA) to authorize and regulate certain governmental electronic surveillance of communications *for foreign intelligence purposes*. See 92 Stat. 1783, 50 U.S.C. § 1801 *et seq.*; 1 D. Kris & J. Wilson, National Security Investigations & Prosecutions §§ 3.1, 3.7 (2d ed. 2012) (hereinafter Kris & Wilson).
>
> [. . .]
>
> In FISA, Congress authorized judges of the Foreign Intelligence Surveillance Court (FISC) to approve electronic surveillance *for foreign intelligence purposes* if there is probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power," and that each of the specific "facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." § 105(a)(3), 92 Stat. 1790; see § 105(b)(1)(A), (b)(1)(B), *ibid.*; 1 Kris & Wilson § 7:2, at 194–195; *id.,* § 16:2, at 528–529.

133 S. Ct. at 1143 (emphasis added).

Under section 1861, the FBI may apply for a FISC order to compel the production of "tangible things," typically from a business. 50 U.S.C. § 1861(a)(1). The application must show that there are "reasonable grounds" to believe the tangible things sought are relevant to an authorized investigation, 50 U.S.C. § 1861(b)(2)(A), and the investigation must "be

conducted under guidelines approved by the Attorney General under Executive Order 12,333." 50 U.S.C. § 1861(a)(2)(A). If and only if the FISC finds that the FBI's application meets the statutory requirements, the FISC "shall enter an ex parte order as requested, or as modified, approving the release of tangible things." 50 U.S.C. § 1861(c)(1).

Executive Order 12,333 establishes rules governing U.S. intelligence activities. Exec. Order No. 12,333, 46 Fed. Reg. 59941 (1981), *as amended by* Exec. Order No. 13,284, 68 Fed. Reg. 4075 (2003), Exec. Order No. 13,355, 69 Fed. Reg. 53593 (2004), and Exec. Order No. 13,470, 73 Fed. Reg. 45325 (2008). "Elements of the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad." Exec. Order No. 12,333 § 2.4. The FBI coordinates all foreign intelligence collection in the United States. *See* Kris & Wilson § 2:7. This includes the NSA's collection of signals intelligence. *See Id.* § 1.7(c)(1). Hence, when NSA seeks business records covered by the 50 U.S.C. § 1861, the FBI files an application with the FISC on the NSA's behalf. *See also* Exec. Order 12,333 § 2.3(b).

II. The FISC Ordered Verizon to Turn Over "All Call Detail Records or 'Telephony Metadata.'"

Through an order from the FISC, the National Security Agency obtained from Verizon Business Network Services, Inc. "telephony metadata" for all domestic phone calls on that company's network. On April 25, 2013, the FISC ordered Verizon to:

> [P]roduce to the National Security Agency (NSA) upon service of this Order, and continue production on an ongoing daily basis thereafter for the duration of this Order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. . . . Telephony metadata includes comprehensive communications routing information, including but not limited to session identifying information (*e.g.*, originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call.

In re Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Bus. Network Serv., Inc. on Behalf of MCI Commc'n Serv., Inc. D/B/A Verizon Bus. Serv., Dkt. No. BR 13-80 at 1-2 (FISA Ct. Apr. 25, 2013) (hereinafter "FISC Order").[2]

---

[2] *Available at* http://www.epic.org/privacy/nsa/Section-215-Order-to-Verizon.pdf.

The "call detail records" referred to in the Verizon Order likely include "[a]ny information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed and the time, location, or duration of any call." 47 C.F.R. § 64.2003 (2012) (defining "call detail information").

Verizon Communications provides services over "America's most advanced fiber-optic network" and operates "America's largest 4G wireless network." *Our Company*, Verizon (2013).[3] It operates the "[n]ation's largest all-fiber network serving residential and small-business customers," handling an "[a]verage of 1 billion calls connected per day." *Fact Sheet*, Verizon (2012).[4] The Verizon enterprise division operates one of the largest telecommunications "backbone networks." *Id*. Verizon provides wireline services in 19 states and the District of Columbia, with revenues of roughly $40 billion in 2012. *Corporate Overview*, Verizon 3 (2012).[5]

---

[3] http://about.verizon.com/index.php/about/our-company.

[4] *Available at* http://about.verizon.com/themes/site_themes/agile_records/images/uploads/Verizon_Corporate_Fact_Sheet.pdf.

[5] http://about.verizon.com/themes/site_themes/agile_records/images/uploads/Verizon_Overview_Presentation_04_29_13.pdf.

The FISC Order, which is classified, was acknowledged and confirmed by President Obama. *See* Remarks on Health Insurance Reform and an Exchange With Reporters in San Jose, California, 2013 Daily Comp. Pres. Doc. 201300397 (June 7, 2013).[6] Senator Diane Feinstein, Chairwoman of the Senate Intelligence Committee, stated that this FISC Order is part of an ongoing electronic communications surveillance program that has been reauthorized since 2007. Charlie Savage, Edward Wyatt & Peter Baker, *U.S. Confirms Gathering of Web Data Overseas*, N.Y. Times, June 7, 2013, at A1. The Verizon Order is set to expire on July 19, 2013, FISC Order at 4. According to Senator Feinstein and other members of the Intelligence Community, the order has been routinely renewed and will likely continue to be renewed.

III. EPIC, a Verizon Customer, Conducts Privileged and Confidential Communications

Petitioner EPIC is a non-profit public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values. EPIC is also a Verizon customer, and has been for the entire period the FISC Order has been in effect. *See* Rotenberg Decl. at 2, Pet. App. 5a. Because the FISC Order compels disclosure of "all call detail records," FISC Order at 2, detailed information about

---

[6] *Available at* http://www.whitehouse.gov/the-press-office/2013/06/07/statement-president.

all of EPIC's telephone communications, including the numbers dialed and when calls occurred, have been disclosed to the NSA.

In furtherance of its mission to protect privacy and advocate for civil liberties, EPIC engages in several activities involving telephonic communications. EPIC files Freedom of Information Act ("FOIA") requests with federal agencies and pursues those requests with litigation as needed. These requests are typically sent via facsimile over EPIC's Verizon business line. EPIC is currently engaged in multiple FOIA lawsuits, including one against the NSA, two against the FBI, one against the Office of the Director of National Intelligence ("ODNI"), and two against the Department of Justice ("DOJ"). *See*, *e.g.*, *EPIC v. DHS*, No. 13-5113 (D.C. Cir. 2013); *EPIC v. FBI*, No. 13-442 (D.D.C. 2013); *EPIC v. CIA*, 12-2053 (D.D.C. 2012); *EPIC v. ODNI*, No. 12-1282 (D.D.C. 2012); *EPIC v. FBI*, No. 12-667 (D.D.C. 2012); *EPIC v. DOJ*, No. 12-127 (D.D.C. 2012); *EPIC v. NSA*, No. 10-196 (D.D.C. 2010); *EPIC v. DOJ*, No. 06-96 (D.D.C. 2006).

EPIC attorneys use EPIC's telephones to conduct privileged attorney-client communications regarding ongoing legal proceedings. EPIC also petitions for, comments on, and litigates federal agency rulemakings under the Administrative Procedure Act. *See, e.g.*, *EPIC v. Dep't of Educ.*, No. 12-327 (D.D.C. 2012). *See also* Rotenberg Decl. at 2, Pet. App. 5a. EPIC's petition initiatives involve communicating telephonically with consumers, advisers, coalition members, and executive and legislative branch officials.

EPIC also engages in policy advocacy through formal and informal consultations with various

parties via telephone. EPIC provides expert advice to Members of Congress regarding oversight and legislation, and consults with federal agencies on regulatory proposals and enforcement. Rotenberg Decl. at 2, Pet. App. 5a. In many cases, discussions with U.S. officials are conducted confidentially to facilitate a deliberative process. In addition, EPIC gives interviews and background briefings with news media, sometimes in a confidential, "off the record" capacity. Rotenberg Decl. at 2, Pet. App. 5a. All of these activities require communication via telephone.

Following the public disclosure of the Verizon Order, EPIC learned that the NSA had obtained vast amounts of call detail information and breached the confidentiality of its privileged and confidential communications.

This petition followed.

REASONS FOR GRANTING THE PETITION

The All Writs Act, 28 U.S.C. § 1651, authorizes the Supreme Court to issue extraordinary writs in its discretion. "To justify granting any such writ, the petition must show that the writ will be in aid of the Court's appellate jurisdiction, that exceptional circumstances warrant the exercise of the Court's discretionary powers, and that adequate relief cannot be obtained in any other form or from any other court." Sup. Ct. R. 20.1. *See also U.S. Alkali Export Ass'n v. United States*, 325 U.S. 196, 201-02 (1945); *De Beers Consol. Mines, Ltd. v. United States*, 325 U.S. 212, 217 (1945).

In this case, the Foreign Intelligence Surveillance Court ("FISC") exceeded its statutory

jurisdiction and as a direct consequence created the exceptional circumstances that warrant mandamus review. The ongoing collection of the domestic telephone records of millions of Americans by the NSA, untethered to any particular investigation, is beyond the authority granted by Congress to the FISC under the FISA. Because of the structure of the FISA and the FISC, EPIC can only obtain relief from this Court.

The Court may grant a petition for mandamus in its discretion, so long as it has jurisdiction over the matter. As the Court described in *Cheney v. U.S. Dist. Court for the Dist. of Columbia*:

> [Mandamus] is a "drastic and extraordinary" remedy "reserved for really extraordinary causes." *Ex parte Fahey*, 332 U.S. 258, 259-260, 67 S.Ct. 1558, 91 L.Ed. 2041 (1947). "The traditional use of the writ in aid of appellate jurisdiction both at common law and in the federal courts has been to confine [the court against which mandamus is sought] to a lawful exercise of its prescribed jurisdiction." *Roche v. Evaporated Milk Assn.*, 319 U.S. 21, 26, 63 S.Ct. 938, 87 L.Ed. 1185 (1943). Although courts have not "confined themselves to an arbitrary and technical definition of 'jurisdiction,' " *Will v. United States*, 389 U.S. 90, 95, 88 S.Ct. 269, 19 L.Ed.2d 305 (1967), "only exceptional circumstances amounting to a judicial 'usurpation of power,' " *ibid.*, or a "clear abuse of discretion," *Bankers Life & Casualty Co. v. Holland*, 346 U.S.

> 379, 383, 74 S.Ct. 145, 98 L.Ed. 106 (1953), "will justify the invocation of this extraordinary remedy," *Will*, 389 U.S., at 95, 88 S.Ct. 269.

542 U.S. 367, 380 (2004). The Court in *Cheney* made clear that three conditions must be satisfied before such an extraordinary writ must issue: (1) the party must have no other adequate means to attain the relief he deserves, (2) the party must satisfy the burden of showing that his right to issuance of the writ is clear and indisputable, and (3) the issuing court must be satisfied that the writ is appropriate under the circumstances. *Id.* at 380-81. Petitioner EPIC satisfies the three conditions set out in *Cheney*.

I. EPIC Cannot Obtain Relief from Any Other Court or Forum

The Court will not grant an extraordinary writ if another avenue of relief remains available. Sup. Ct. R. 20.1. However, the relief EPIC seeks, a writ vacating the unlawful FISC Order, cannot be granted by any other court. The lower federal courts have no jurisdiction to hear EPIC's appeal, and the Court has made clear that mandamus relief is available in such unique circumstances. *See U.S. Alkali Export Ass'n*, 325 U.S. at 202 (finding that a writ in aid of appellate jurisdiction must be to the Supreme Court where it has sole appellate jurisdiction).[7]

---

[7] *See also In re Blodgett*, 502 U.S. 236, 240 (1992) (denying mandamus where the state could have asked the Court of Appeals to vacate or modify its order); *Will v. United States*, 389 U.S. 90, 96 (1967) (noting that government appeals are disfavored in criminal cases, but that

The FISC and Foreign Intelligence Surveillance Court of Review ("Court of Review") only have jurisdiction to hear petitions by the Government or recipient of the FISC Order, and neither party to the order represents EPIC's interests. Other federal courts have no jurisdiction over the FISC, and thus cannot grant the relief that EPIC seeks.

A. EPIC Cannot Seek Relief from the FISC or Court of Review.

The plain terms of the Foreign Intelligence Surveillance Act and the rules of the FISC bar EPIC from seeking relief before the FISC or Court of Review. The FISC may only review business record orders upon petition from the recipient or the Government. 50 U.S.C. § 1861(f)(2)(A)(i); Foreign Intelligence Surveillance Ct. R. 33(a). *See also* Kris & Wilson § 19:7.[8]

Further review of FISC orders and denials is also limited. Only the Government or the recipient of a business record order may petition for an *en banc* rehearing by the FISC. 50 U.S.C. § 1803(a)(2)(A); Foreign Intelligence Surveillance Ct. R. 46. The Court of Review only has jurisdiction to review denials of business record applications, 50 U.S.C. §

---

mandamus relief is allowed in certain narrow circumstances).

[8] In fact, before the enactment of the USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006), "the statute appeared to contemplate that only the government could appear before the FISC." Kris & Wilson § 19:7.

1803(b), and decisions to affirm, modify, or set aside business record orders after a petition by the Government or the recipient. 50 U.S.C. § 1861(f)(3). *See* Kris & Wilson § 5:7.[9]

EPIC is not the recipient of a Business Records order under § 1861, but rather EPIC's communications are subject to the FISC Order. As a result, the FISC and Court of Review have no jurisdiction to grant EPIC the relief it seeks.

This Court can grant mandamus relief without causing piecemeal litigation. Mandamus should not be a substitute for an interlocutory appeal. *Will*, 389 U.S. at 97. The general policy against piecemeal appeals underlies much of this Court's mandamus jurisprudence. *Id*. at 96. Appellate review is ideally sought after a final judgment has been rendered. *See* Judiciary Act of 1789, §§ 21, 22, 25, 1 Stat. 73, 83, 84, 85 (1789). This case would not result in piecemeal litigation because EPIC seeks review of a final order of the FISC.

B. No Other Court Can Grant EPIC the Relief It Seeks.

No other court has the power to vacate the FISC Order. Other federal and state trial and appellate courts have no jurisdiction over the FISC. *See generally* 50 U.S.C. § 1803. Under the All Writs

---

[9] Both the FISC and the Court of Review have the authority to issue a stay or modify an order during the pendency of any review by the Supreme Court, while an appeal is pending before the Court of Review, or while the FISC is conducting a rehearing. 50 U.S.C. § 1803(f)(1).

Act, federal courts are only empowered to issue writs "in aid of their respective jurisdictions." 28 U.S.C. § 1651(a). *Accord Moye v. Clerk, DeKalb Cnty Super. Ct.*, 474 F.2d 1275, 1275-76 (5th Cir. 1973) (holding that although the writ of mandamus was abolished by Fed. R. Civ. P. 81(b), federal district courts may still issue writs in aid of their jurisdiction). The FISC order is outside the jurisdiction of federal district and circuit courts. Only this Court, the Court of Review, and the FISC are empowered to consider petitions to affirm, modify, or set aside a FISA Business Records order. 50 U.S.C. § 1861(f)(3). As a result, EPIC cannot petition an inferior federal court to vacate the unlawful FISC Order.

Any alternative relief that EPIC could seek is directly limited by this order. Both Verizon and the government agents executing this order are granted immunities based on the presumed validity of a court order. *See* 50 U.S.C. § 1861(e). Furthermore, the parties to the FISC Order do not serve EPIC's interests and their right to petition for review does not provide adequate oversight to the judge's unlawful FISC Order. EPIC can only prevent the application of this unlawful order by having it vacated by this Court.

II. The FISC Order Exceeded the Scope of the FISC's Jurisdiction Under the FISA

Writs of mandamus in aid of appellate jurisdiction are traditionally used to confine a lower court to the lawful exercise of its jurisdiction. *Cheney*, 542 U.S. at 380. Such a jurisdictional correction is required here: the FISC issued an order requiring disclosure of records for all telephone communications "wholly within the United States,

including local telephone calls." FISC Order at 2. The Business Records provision does not enable this type of domestic programmatic surveillance.

Specifically, the statute requires that production orders be supported by "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation. . . ." 50 U.S.C. § 1861(b)(2)(A). It is simply unreasonable to conclude that all telephone records *for all Verizon customers in the United States* could be relevant to an investigation. Thus, the FISC simply "ha[d] no judicial power to do what it purport[ed] to do." *De Beers,* 325 U.S. at 217.

A. Mandamus Aids the Court's Appellate Jurisdiction When It Prevents a Lower Court from Exceeding Its Lawful Authority.

A petition for a writ of mandamus under 28 U.S.C. § 1651(a) "must show that the writ will be in aid of the Court's appellate jurisdiction. . . ." Sup. Ct. R. 20.1. "The traditional use of the writ in aid of appellate jurisdiction both at common law and in the federal courts has been to confine [the court against which mandamus is sought] to a lawful exercise of its prescribed jurisdiction." *Cheney,* 542 U.S. at 380 (quoting *Roche v. Evaporated Milk Ass'n*, 319 U.S. 21, 26 (1943)). Jurisdictional errors are not measured against "an arbitrary and technical definition of 'jurisdiction,'" *Will*, 389 U.S. at 95. Rather, petitioners need to show that there was a "clear abuse of discretion," *Bankers Life & Cas. Co. v. Holland*, 346 U.S. 379, 383 (1953), or judicial "usurpation of power." *De Beers*, 325 U.S. at 217.

Thus, in *De Beers* the Court issued a writ to stop a district court from sequestering property when it was "not authorized" by the antitrust statute under which the case was brought; the court "ha[d] no judicial power to do what it purport[ed] to do." 325 U.S. at 217-23. *See also U.S. Alkali Export Ass'n v. United States*, 325 U.S. 196, 204 (1945) (review of district court appropriate to avoid creating a "frustration of the functions which Congress" intended); *Ex parte Republic of Peru*, 318 U.S. 578, 586-90 (1943) (mandamus warranted when a district court exceeded the scope of its jurisdiction by proceeding in rem against a foreign steamship).

A court can exceed its jurisdiction by going beyond the bounds of its statutory instructions, not just by engaging in wholly unauthorized activity. In *Mallard v. U.S. Dist. Court for the S. Dist. of Iowa*, mandamus was merited because the district court "did not lawfully exercise its jurisdiction" when it appointed an attorney to represent an indigent client, despite only being authorized to "request" the representation. 490 U.S. 296, 308-09 (1989). Similarly, in *Schlagenhauf v. Holder*, the Court prevented a district court from "disregarding plainly expressed [statutory] limitations" by ordering a physical and mental examination not justified by the Federal Rules of Civil Procedure. 379 U.S. 104, 121 (1964).

B. The FISC Lacks the Legal Authority to Order Programmatic Domestic Surveillance Under 50 U.S.C. § 1861.

The FISC exceeded its statutory authorization under the FISA when it ordered Verizon to disclose all domestic telephone communications records,

without limitation, to the NSA on an ongoing basis. Under the Business Records provision, the FBI may make an application to the FISC for an order requiring:

> [T]he production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

50 U.S.C. § 1861(a)(1). If the FBI's application meets the statutory requirements, the FISC "shall enter an ex parte order as requested, or as modified, approving the release of tangible things." 50 U.S.C. § 1861(c)(1). The FISC's responsibility to ensure adequacy of the application "is not merely a ministerial requirement; if the FISC concludes that the statement of facts does *not* make the necessary showing of relevance, it must deny the application." Kris & Wilson § 19:3.

The statute requires that the FBI's statement of facts show "that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2). . . ." 50 U.S.C. § 1861(b)(2)(A). An authorized investigation requires a factual predicate, whereas a

threat assessment does not.[10] *See Attorney General's Guidelines for Domestic FBI Operations*, U.S. Dep't of Justice, 17-18 (2008).[11] "Reasonable grounds" is not defined in the statute, but according to Kris & Wilson it has been treated as equivalent to "reasonable suspicion." *See, e.g.*, *United States v. Banks*, 540 U.S. 31, 36 (2003); *United States v. Henley*, 469 U.S. 221, 227 (1985); *United States v. Brignoni-Ponce*, 422 U.S. 873, 881-82 (1975); Kris & Wilson § 19:3. "Reasonable suspicion" requires a showing of "specific and articulable facts, which, taken together with rational inferences from those facts, reasonably warrant" intrusion into a suspect's privacy. *Terry v. Ohio*, 392 U.S. 1, 21 (1968). Given that the FISC Order commands disclosure of *all* domestic telephone records, it is acutely implausible that the FBI alleged specific and articulable facts about each of Verizon's millions of customers.

What makes a tangible thing "relevant" to an authorized investigation is likewise not clearly delineated in the statute. However, in accordance with the foreign intelligence purposes of FISA, the Act says that tangible things are "presumptively relevant" if they

> pertain to – (i) a foreign power or an agent of a foreign power; (ii) the

---

[10] Simply acquiring a haystack to go looking for a needle is a threat assessment. An authorized investigation would be specifically targeted on an identified needle based on a factual predicate.

[11] *Available at* http://www.justice.gov/ag/readingroom/guidelines.pdf.

> activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation[.]

50 U.S.C. § 1861(b)(2)(A). Common sense dictates that the vast majority of Verizon's customers will not fall into any of these three categories. Consequently, the vast majority of the telephone records conveyed to the NSA will not be presumptively relevant. The burden is therefore on the FBI to show, with specific and articulable facts, why those records are in fact relevant and should be included in the production order.

Moreover, the scope of the request cannot simply encompass all call records in the database. To define the scope of the records sought as "everything" nullifies the relevance limitation in the statute. If law enforcement has "everything," there will always be some subset of "everything" that is relevant to something. At that level of breadth, the relevance requirement becomes meaningless. *See Reiter v. Sonotone Corp.*, 442 U.S. 330, 339 (1979) ("In construing a statute we are obliged to give effect, if possible, to every word Congress used."). In addition to showing a sufficient factual predicate, the FBI's investigation must also "be conducted under guidelines approved by the Attorney General under Executive Order 12333. . . ." 50 U.S.C. § 1861(a)(2)(A). The Executive Order emphasizes the need to limit the scope of domestic surveillance. "The United States Government has a solemn obligation,

and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law." Exec. Order No. 12,333 § 1.1(b).

In particular, Executive Order 12,333 requires intelligence agencies to "use the least intrusive collection techniques feasible within the United States or directed at U.S. persons abroad." *Id*. at § 2.4. The unbounded collection and review of the call detail records of all Americans is plainly not "the least intrusive technique feasible." It is difficult to conceive of any surveillance technique more intrusive than acquiring all communications records on all persons concerning all matters.

Finally, reading § 1861 in the context of the FISA as a whole, it becomes clear that this section is not meant to authorize the ongoing programmatic collection of telephone records. *See K Mart Corp. v. Cartier, Inc.*, 486 U.S. 281, 291 (1988) ("In ascertaining the plain meaning of the statute, the court must look to the particular statutory language at issue, as well as the language and design of the statute as a whole."). While section 1861 authorizes the requisition of "tangible things," sections 1841-42 authorize the use of "[p]en registers and trap and trace devices for foreign intelligence and international terrorism investigations." A pen register is a device or process that "records or decodes dialing, routing, addressing, or signaling information" of electronic communications. 18 U.S.C. § 3127(3). A trap and trace device is a device or process that "captures the incoming electronic or

other impulses which identify the originating number or other dialing, routing addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." 18 U.S.C. § 3127(4).

Use of pen registers and trap and trace devices is the classic technique that this Court has recognized for the collection of call detail records, which were originally simply telephone numbers dialed. *See Smith v. Maryland*, 442 U.S. 735 (1979). Pen registers and trap and trace devices are also used for present and future monitoring of communications, as opposed to historical record collection. They are the sorts of devices and methods one would use to capture telephony metadata. To the extent that Congress intended to allow the FISC to order ongoing domestic communications surveillance for foreign intelligence purposes, such orders should be rooted in section 1842 concerning pen registers and trap and trace devices, not section 1861's tangible things provisions.[12]

---

[12] Chairman Sensenbrenner, an original co-sponsor of the Patriot Act, stated recently that Congress never intended or understood the Business Records section to authorize bulk surveillance of Americans' activities. "Congress intended to allow the intelligence communities to access targeted information for specific investigations. How can every call that every American makes or receives be relevant to a specific investigation?" Rep. Jim Sensenbrenner, *This Abuse of the Patriot Act Must End*, The Guardian, June 9, 2013, http://www.guardian.co.uk/commentisfree/2013/jun/09/abuse-patriot-act-must-end.

The FISC order for the ongoing production of detailed telephone records, concerning solely domestic communications, went far beyond the authority set out in the Act. The FISC is required by FISA to approve applications that meet the statutory requirements and deny applications that fail to meet those requirements. 50 U.S.C. § 1861(c)(1). By approving this statutorily deficient application, the FISC exceeded its lawful authority.

III. The FISC Order Creates Exceptional Circumstances Warranting Mandamus.

A writ of mandamus may issue when "exceptional circumstances warrant the exercise of the Court's discretionary powers." Sup. Ct. R. 20.1. There are no formal bounds to what constitutes an exceptional circumstance; the Court's mandamus discretion is quite broad. *See* Steven Wisotsky, *Extraordinary Writs: "Appeal" by Other Means*, 26 Am. J. Trial Advoc. 577, 583 (2003); James E. Pfander, *Jurisdiction-Stripping and the Supreme Court's Power to Supervise Inferior Tribunals*, 78 Tex. L. Rev. 1433, 1494-97 (2000). Mandamus is also appropriate where the case presents an "issue of first impression" involving a "basic and undecided problem," especially on an important issue like foreign intelligence surveillance that is rarely reviewed by the Supreme Court. *United States v. U.S. Dist. Court for Eastern Dist. of Mich., Southern Division (Keith)*, 444 F.2d 651, 655-56 (6th Cir. 1971), *aff'd*, 407 U.S. 297 (1972) (quoting *Schlagenhauf v. Holder*, 379 U.S. 104, 110 (1964)).

This case involves a far-reaching FISC order that gives the NSA access to the telephone call records of millions of Americans on an ongoing basis.

Such a broad grant of executive power is not permitted under the FISA and cannot be justified by a non-particularized connection to general national security threats. "Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent." *Olmstead v. United States*, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting).[13]

A. Telephony Metadata Reveals Significant Private Information About EPIC and Millions of Other Americans.

Telephony metadata can be directly linked to each user's identity and reveal their contacts, clients, associates, and even the physical location. The FISC Order specifies that "[t]elephony metadata includes comprehensive communications routing information, including but not limited to session identifying information (*e.g.,* originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call." FISC Order at 2.

Routing information refers to "the path or method to be used for establishing telephone

---

[13] Even admirable ends do not justify the creation of a panopticon. *See Maryland v. King*, 569 U.S. __, 133 S.Ct. 1958, 1989 (2013) (Scalia, J., dissenting) ("Solving unsolved crimes is a noble objective, but it occupies a lower place in the American pantheon of noble objectives than the protection of our people from suspicionless law-enforcement searches.").

connections or forwarding messages." Telecomm. Indus. Ass'n, *Routing*, Glossary of Telecommunications Terms.[14] Routing information therefore encompasses all information about the path of the telephone call, including the cell sites or switching stations used to complete the call. *See generally*, Ray Horak, *Telecommunications and Data Communications Handbook* 200-247; 550-600 (2007). IMSI and IMEI numbers are both unique identifiers related to mobile telephony. The IMSI number is a unique number used to identify a subscriber to a mobile network. ATIS – IMSI Oversight Council, *Frequently Asked Questions*.[15] The IMEI number is a unique number assigned to a mobile device by the device manufacturer and used to identify the device on the network. CTIA – The Wireless Ass'n, *Wireless Glossary of Terms* (Oct. 2012).[16] Finally, "trunk identifier" could refer to a number that uniquely identifies a group of communications channels or to the "trunk code" used to identify the home network or area inside a country where a call is to be routed. *See* Tarmo Anttalainen, *Introduction to Telecommunications Network Engineering* 32 (2d. ed.

---

[14] *Available at* http://www.tiaonline.org/resources/telecom-glossary (search for "routing") (last visited July 1, 2013).

[15] http://www.imsiadmin.com/imsi_faq.cfm (last visited July 1, 2013).

[16] http://www.ctia.org/media/industry_info/index.cfm/AID/10409.

2003); Telecomm. Indus. Ass'n, *Trunk*, Glossary of Telecommunications Terms.[17]

Because the routing information details the path taken by a call, it can be used to identify the location of the parties to the call. The connections made between an individual's mobile phone and the antennas in a service provider's network can be used to track location over time. *See* Junhui Zhao & Xueue Zhang, *Location-Based Services Handbook: Wireless Location Technology in Location-Based Services* § 2.2.1 (Syed A. Ahson & Mohammad Ilyas eds., 2011); Axel Küpper, *Location-Based Services: Fundamentals and Operation* § 6.2.1 (2006).

The FISC Order also compels disclosure of personally identifiable information. Telephone numbers, IMSI numbers, and IMEI numbers are unique and can be used to identify individuals. The NSA maintains a database of "telephone numbers and electronic communications accounts / addresses / identifiers that NSA has reason to believe are being used by United States Persons." *Procedures used by the Nat'l Sec. Agency for Targeting Non-U.S. Persons Reasonably Believed to be Located Outside the U.S. to Acquire Foreign Intelligence Info. Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended*, Nat'l Sec. Agency, at 3 (FISA Ct. filed Jul. 29, 2009).[18] These numbers collected under

---

[17] *Available at* http://www.tiaonline.org/resources/telecom-glossary (search for "trunk") (last visited July 1, 2013).

[18] *Available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/716633/exhibit-a.pdf.

the FISC Order can be easily matched with the records maintained in the NSA identifying database. In fact, the NSA uses this matching process to "prevent the inadvertent targeting of a United States person" under directives issued pursuant to Section 702 of FISA. *Id.*

Because telephone numbers identify individuals, they are protected as personal information under federal law. *See, e.g.,* 15 U.S.C. § 6501(8)(A)-(E) (2012) (including "telephone number" within the definition of personal information); 18 U.S.C. § 2725(3) (2012), (including "telephone number" within the definition of personal information). *See also* 47 U.S.C. § 222(h)(1)(A) (2012) (defining "customer proprietary network information" as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service. . . .").

The telephony metadata obtained under the FISC Order is used by the NSA to create maps of an individual's social connections. These social maps contain information about users private contacts and associations. This process is referred to as "contact chaining," and it is used to structure and catalog the telephony metadata held by the NSA. *See* Memorandum from Kenneth Wainstein, Assistant Att'y Gen., Dep't of Justice, to the Att'y Gen. of the United States, at 2 (Nov. 20, 2007).[19] Contact chaining allows the agency to "automatically identify

---

[19] *Available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/717974/nsa-memo.pdf.

not only the first tier of contacts made by the seed telephone number or e-mail address, but also the further contacts made by the first tier of telephone numbers or e-mail addresses and so on." *Id.* at 13. So if the NSA was investigating Bob's telephone records, and saw he called Jane, the NSA would then collect and examine all of Jane's telephone records. If they saw that Jane called Steve, they would then collect and examine all of Steve's telephone records. Contact chaining was specifically designed as a means to analyze the communications metadata of U.S. persons. *Id.* at 2.[20] But this process also gives rise to combinatorial explosion, permitting the creation of enormous data sets containing personal information completed unrelated to the purpose of the investigation.

The practical use of telephone numbers to identify individuals is well understood. In 2006, Senator Joe Biden told CBS News that "I don't have to listen to your phone calls to know what you're doing. If I know every single phone call you made, I'm able to determine every single person you talked to. I can get a pattern about your life that is very, very intrusive." *The Early Show* (CBS News broadcast

---

[20] *See also United States v. Jones*, 567 U.S. ___, 132 S.Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.").

May 12, 2006).[21] And if all call record information is relevant under the FISA, then other categories of business records could also be obtained in bulk under the statute.

B. EPIC is in Active Litigation Against the Very Agencies Tracking EPIC's Privileged Attorney-Client Communications.

The FISC Order mandates that Verizon produce data about EPIC's confidential attorney-client relationships and other privileged information. The privacy of such communications is essential to the "public interests in the observance of law and administration of justice." *Upjohn v. United States*, 449 U.S. 383, 389 (1981). *See also* Kris & Wilson § 19:10 (noting that a tangible things order could be characterized as "unlawful" if it sought privileged communications).

EPIC frequently files Freedom of Information Act ("FOIA") requests with federal agencies and pursues those requests with litigation when necessary. At present, EPIC is in litigation with both the NSA and FBI, the two agencies responsible for tracking Americans' private communications under this order. *EPIC v. FBI*, No. 13-442 (D.D.C. 2013); *EPIC v. FBI*, No. 12-667 (D.D.C. 2012); *EPIC v. NSA*, No. 10-196 (D.D.C. 2010). Additionally, EPIC has ongoing FOIA lawsuits against other elements of the Intelligence Community, including the Office of the Director of National Intelligence and the Central

---

[21] *Available at* http://www.cbsnews.com/video/watch/?id=1613914n.

Intelligence Agency. *EPIC v. ODNI*, No. 12-1282 (D.D.C. 2012); *EPIC v. CIA*, 12-2053 (D.D.C. 2012). At the FISC's command, Verizon is turning over EPIC's privileged information to the very parties capable of exploiting that information.[22] The court's order hampers EPIC's ability to deliberate and develop litigation strategies "free from the consequences or the apprehension of disclosure." *Hunt v. Blackburn*, 128 U.S. 464, 470 (1888). *See also Weatherford v. Bursey*, 429 U.S. 545, 554 n.4 (1977) (noting that government surveillance of attorney-client communications threatens the "inhibition of free exchanges between defendant and counsel.").

Courts consider a threat to attorney-client communications an exceptional circumstance and have issued writs of mandamus to vacate production orders implicating privileged information. *See, e.g.*, *In re BankAmerica Corp. Sec. Litig.*, 270 F.3d 639 (8th Cir. 2001) (attorney-client); *Admiral Ins. Co. v. U.S. Dist. Court for the Dist. of Ariz.*, 881 F.2d 1486 (9th Cir. 1989) (attorney-client); *In re Fink*, 876 F.2d 84 (11th Cir. 1989) (doctor-patient). In this case, the FISC issued a blanket order for all domestic telephone records. Such a boundless order sweeps up not just communications protected by attorney-client privilege, but also those falling under marital communications privilege, psychiatrist-patient

---

[22] *See also Clapper v. Amnesty Int'l USA*, 568 U.S. __, 133 S.Ct. 1138, 1154 (2013) (stating that an attorney could have standing for a claim alleging unlawful FISA surveillance of attorney-client communications).

privilege, accountant-client privilege, and clergy-penitent privilege.

C. EPIC Confidentially Communicates with Members of Congress, Agency Officials, Journalists, and Others to Further its First Amendment-Protected Advocacy.

EPIC's ability to engage in open dialogue with the public, coalition members, and colleagues in government, non-government, and the private sector is protected by the First Amendment doctrines of freedom of association and freedom of speech. As described above, EPIC communicates regularly with coalition groups, international organizations, consumers, and government representatives. Members of EPIC's staff give telephone interviews to reporters and journalists, speak to members of Congress who seek expert opinions on privacy issues, and consult with other advocates about privacy law and policy. Many of these conversations are conducted with the expectation that they will remain confidential, to protect the deliberative process of those with whom EPIC consults.

This Court has frequently recognized the importance of preserving the First Amendment rights of advocacy groups. In *Gibson v. Florida Legislative Investigation Committee,* this Court ruled, "[t]he First and Fourteenth Amendment rights of free speech and free association are fundamental and highly prized, and 'need breathing space to survive.'" 372 U.S. 539, 892 (1963), citing *N.A.A.C.P. v. Button*, 371 U.S. 415, 433 (1963). In *N.A.A.C.P. v. Alabama*, this Court explained why the protection of privacy is of Constitutional concern for advocacy organizations:

> [I]t is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute an effective restraint on freedom of association as the forms of governmental action in the cases above were thought likely to produce upon the particular constitutional rights there involved.. This Court has recognized the vital relationship between freedom to associate and privacy in one's associations. . . . Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.

357 U.S. 449, 462 (1958). Because of the confidential, candid nature of EPIC's consultations with various parties, NSA's surveillance chills EPIC's ability to advocate. "Freedoms such as these are protected not only against heavy-handed frontal attack, but also from being stifled by more subtle governmental interference." *Id.* at 523. *See also Laird v. Tatum*, 408 U.S. 1, 11, (1972) ("[C]onstitutional violations may arise from the deterrent, or 'chilling,' effect of governmental [efforts] that fall short of a direct prohibition against the exercise of First Amendment rights."). A non-profit advocacy group engaging in political speech must be able to have private telephone communications without fear of constant monitoring by the government.

Given the vital importance of First Amendment protections for advocacy groups, appellate courts have recognized government threats

to free speech and association to constitute an "extraordinary circumstance" warranting mandamus review. *See*, *e.g., Perry v. Schwarzenegger*, 591 F.3d 1126 (9th Cir. 2009) (mandamus to protect campaign strategy communications from discovery, due to their effect of discouraging exercise of the right to associate with an advocacy group); *CBS Inc. v. Young*, 522 F.2d 234 (6th Cir. 1975) (mandamus granted to protect the free speech rights of both student demonstrators and the national guard); *Chase v. Robson*, 435 F.2d 1059 (7th Cir. 1970) (mandamus to protect free speech rights of litigants).

By ordering surveillance of all Verizon customers, the FISC permitted the NSA to gather the metadata of EPIC's conversations with consumers, advisors and advisees, donors, other privacy advocates, Members of Congress, agency officials, and journalists. The government need not stage a "heavy-handed frontal attack" against EPIC's communications in order to threaten its right to free speech and association. *Bates v. City of Little Rock*, 361 U.S. 516, 523 (1980). The NSA does not need the contents of communications to stifle EPIC's advocacy. The metadata alone is sufficient to identify who has been talking to EPIC and to chill those communications and associations. *See United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse.").

D. The FISC Order Compels Disclosure of Judicial and Congressional Communications, Raising Separation of Powers Concerns.

The FISC Order threatens the autonomy of the Legislative and Judicial branches by authorizing the Executive to collect the telephone communication records of Members of Congress and federal judges. The Framers determined that the creation of three coequal branches of government was "essential to the preservation of liberty." *Mistretta v. United States*, 488 U.S. 361, 380 (1989). Accordingly, the Constitution prohibits efforts by one branch to control, interfere with, or unduly burden the exercise of the constitutionally assigned functions of another branch. *See Clinton v. Jones*, 520 U.S. 681, 701 (1997) ("We have recognized that '[e]ven when a branch does not arrogate power to itself . . . the separation-of-powers doctrine requires that a branch not impair another in the performance of its constitutional duties." (citation omitted)); *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 509 (1977) (Appealing to the "necessity of maintaining each of the three general departments of government entirely free from the control or coercive influence, direct or indirect, of either of the others." (quoting *Humphrey's Ex'r v. United States*, 295 U.S. 602, 629-30 (1935)).

Here, the Executive's collection of all Verizon call data unduly burdens the functioning of the other two coordinate branches. The Constitution vests "[a]ll legislative Powers herein granted" in the Congress of the United States, U.S. Const. Art. I, § 1, and "[t]he judicial Power" in "one supreme Court, and in such inferior Courts as the Congress may from time to

time ordain and establish." U.S. Const. Art. III, § 1. In order to exercise the legislative power, members of Congress depend upon the ability to communicate frankly with staff members and with constituents, many of whom are Verizon customers. *See, e.g., United States v. Ford*, 830 F.2d 596, 601 (6th Cir. 1987) (holding that separation of powers protects the integrity of "political communication between a congressman and his constituents").

Similarly, in order to exercise the judicial power, members of the federal judiciary need to communicate openly with each other and with staff members, attorneys, and litigants. *See, e.g.*, *Matter of Certain Complaints Under Investigation by an Investigating Comm. of Judicial Council of Eleventh Circuit*, 783 F.2d 1488, 1519-20 (11th Cir. 1986) ("Judges, like Presidents, depend upon open and candid discourse with their colleagues and staff to promote the effective discharge of their duties. . . . Confidentiality helps protect judges' independent reasoning from improper outside influences."). The Executive Branch is currently collecting metadata for *all calls* made by judges who are Verizon customers or who communicate with Verizon customers. As the Court has recognized, surveillance can impair open communication and intellectual exploration. This interference with the communicative freedom of members of the judiciary and legislature "impair[s these branches] in the performance of [their] constitutional duties," *Clinton v. Jones*, 520 U.S. 681, 701 (1997), and thereby threatens the separation of powers. Thus, mandamus is warranted to remedy the interference.

CONCLUSION

For the foregoing reasons, Petitioner respectfully asks this Court to grant the petition for a writ of mandamus and prohibition, or, in the alternative, the petition for a writ of certiorari.

Respectfully submitted,

MARC ROTENBERG
Counsel of Record
ALAN BUTLER*
DAVID JACOBS**
DAVID BRODY***
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

July 8, 2013

**Member of the bar of the District of Columbia*

***Member of the bar of New York*

****Member of the bar of California*

APPENDIX A

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.
Docket Number: BR 13-80

IN RE APPLICATION OF THE FEDERAL BUREAU OF INVESTIGATION FOR AN ORDER REQUIRING THE PRODUCTION OF TANGIBLE THINGS FROM VERIZON BUSINESS NETWORK SERVICES, INC. ON BEHALF OF MCI COMMUNICATION SERVICES, INC. D/B/A VERIZON BUSINESS SERVICES.

SECONDARY ORDER

This Court having found that the Application of the Federal Bureau of Investigation (FBI) for an Order requiring the production of tangible things from Verizon Business Network Services, Inc. on behalf of MCI Communication Services Inc., d/b/a Verizon Business Services (individually and collectively "Verizon") satisfies the requirements of 50 U.S.C. § 1861,

IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production on an ongoing daily basis thereafter for the duration of this Order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by Verizon for

communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. This Order does not require Verizon to produce telephony metadata for communications wholly originating and terminating in foreign countries. Telephony metadata includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer.

IT IS FURTHER ORDERED that no person shall disclose to any other person that the FBI or NSA has sought or obtained tangible things under this Order, other than to: (a) those persons to whom disclosure is necessary to comply with such Order; (b) an attorney to obtain legal advice or assistance with respect to the production of things in response to the Order; or (c) other persons as permitted by the Director of the FBI or the Director's designee. A person to whom disclosure is made pursuant to (a), (b), or (c) shall be subject to the nondisclosure requirements applicable to a person to whom an Order is directed in the same manner as such person. Anyone who discloses to a person described in (a), (b), or (c) that the FBI or NSA has sought or obtained tangible things pursuant to this Order shall notify such person of the

nondisclosure requirements of this Order. At the request of the Director of the FBI or the designee of the Director, any person making or intending to make a disclosure under (a) or (c) above shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

IT IS FURTHER ORDERED that service of this Order shall be by a method agreed upon by the Custodian of Records of Verizon and the FBI, and if no agreement is reached, service shall be personal.

-- Remainder of page intentionally left blank. --

This authorization requiring the production of certain call detail records or "telephony metadata" created by Verizon expires on the 19th day of July, 2013, at 5:00 p.m., Eastern Time.

Signed 04-25-2013 P02:26 Eastern Time

/s/ ROGER VINSON

Roger Vinson

Judge, United States Foreign Intelligence Surveillance Court

/s/ I, Beverly C. Queen, Chief Deputy Clerk, FISC, certify that this document is a true and correct copy of the original.

APPENDIX B

DECLARATION OF MARC ROTENBERG, PRESIDENT OF EPIC

---

1. My name is Marc Rotenberg. All statements made herein are true and based on my personal knowledge.
2. I am the President of the Electronic Privacy Information Center ("EPIC").
3. I have been employed by EPIC since 1994.
4. EPIC is a non-profit public interest research center founded in 1994 to focus public attention on emerging civil liberties and privacy issues.
5. EPIC's office is located at 1718 Connecticut Ave., NW, Suite 200, Washington, DC, 20009.
6. EPIC maintains several websites, including www.epic.org, www.privacy.org, thepublicvoice.org, www.privacycoalition.org, and www.indefenseoffreedom.org.
7. EPIC employs attorneys and other staff, who investigate and litigate issues related to privacy law, the Administrative Procedure Act ("APA"), and the Freedom of Information Act ("FOIA").
8. EPIC employs nine attorneys, including myself.
9. EPIC files and pursues FOIA requests with federal agencies, including the National Security Agency ("NSA"), the Federal Bureau of Investigation, the Office of the Director of National Intelligence, and the Department of Justice, among others.

10. EPIC files and pursues APA rulemaking petitions with federal agencies, including the NSA and the Department of Homeland Security, among others.
11. EPIC routinely engages in APA and FOIA litigation against federal government agencies.
12. EPIC consults, often confidentially, with Members of Congress, state legislators, and federal and state officials about privacy law and open government issues.
13. EPIC gives interviews to journalists, sometimes in an "off the record" and confidential capacity.
14. EPIC's office contains telephones and a facsimile machine that EPIC's attorneys and staff use for the above activities.
15. EPIC's attorneys often use the telephones to conduct confidential and/or privileged communications related to active litigations.
16. EPIC's attorneys often transmit confidential and/or privileged drafts of attorney work product via facsimile.
17. EPIC is currently a Verizon telephone customer and has been since prior to April 2013.
18. I declare under penalty of perjury that the foregoing is true and correct. Executed on July 2, 2013.

/s/ *Marc Rotenberg*

Marc Rotenberg

President, EPIC

APPENDIX C

1. U.S. Const. Art. I, § 1 provides:

All legislative Powers herein granted shall be vested in a Congress of the United States, which shall consist of a Senate and House of Representatives.

2. U.S. Const. Art. III, § 1 provides:

The judicial Power of the United States, shall be vested in one supreme Court, and in such inferior courts as the Congress may from time to time ordain and establish. The Judges, both of the supreme and inferior Courts, shall hold their offices during good Behaviour, and shall, at stated Times, receive for their Services, a Compensation, which shall not be diminished during their Continuance in Office.

3. 50 U.S.C. 1861 provides:

Access to certain business records for foreign intelligence and international terrorism investigations

(a) Application for order; conduct of investigation generally

(1) Subject to paragraph (3), the Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a

United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

(2) An investigation conducted under this section shall—

(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and

(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(3) In the case of an application for an order requiring the production of library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person, the Director of the Federal Bureau of Investigation may delegate the authority to make such application to either the Deputy Director of the Federal Bureau of Investigation or the Executive Assistant Director for National Security (or any successor position). The Deputy Director or the Executive Assistant Director may not further delegate such authority.

(b) Recipient and contents of application

Each application under this section—

(1) shall be made to—

(A) a judge of the court established by section 1803 (a) of this title; or

(B) a United States Magistrate Judge under chapter 43 of title 28, who is publicly designated by the Chief Justice of the United States to have

the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and

(2) shall include—

(A) a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, such things being presumptively relevant to an authorized investigation if the applicant shows in the statement of the facts that they pertain to—

(i) a foreign power or an agent of a foreign power;

(ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or

(iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation; and

(B) an enumeration of the minimization procedures adopted by the Attorney General under subsection (g) that are applicable to the retention and dissemination by the Federal Bureau of Investigation of any tangible things to be made available to the Federal Bureau of Investigation based on the order requested in such application.

(c) Ex parte judicial order of approval

(1) Upon an application made pursuant to this section, if the judge finds that the application meets the requirements of subsections (a) and (b), the judge shall enter an ex parte order as requested, or as modified, approving the release of tangible things. Such order shall direct that minimization procedures adopted pursuant to subsection (g) be followed.

(2) An order under this subsection—

(A) shall describe the tangible things that are ordered to be produced with sufficient particularity to permit them to be fairly identified;

(B) shall include the date on which the tangible things must be provided, which shall allow a reasonable period of time within which the tangible things can be assembled and made available;

(C) shall provide clear and conspicuous notice of the principles and procedures described in subsection (d);

(D) may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things; and

(E) shall not disclose that such order is issued for purposes of an investigation described in subsection (a).

(d) Nondisclosure

(1) No person shall disclose to any other person that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to an order under this section, other than to—

(A) those persons to whom disclosure is necessary to comply with such order;

(B) an attorney to obtain legal advice or assistance with respect to the production of things in response to the order; or

(C) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

(2)

(A) A person to whom disclosure is made pursuant to paragraph (1) shall be subject to the nondisclosure requirements applicable to a person to whom an order is directed under this section in the same manner as such person.

(B) Any person who discloses to a person described in subparagraph (A), (B), or (C) of paragraph (1) that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to an order under this section shall notify such person of the nondisclosure requirements of this subsection.

(C) At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under subparagraph (A) or (C) of paragraph (1) shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

(e) Liability for good faith disclosure; waiver

A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a

waiver of any privilege in any other proceeding or context.

(f) Judicial review of FISA orders

(1) In this subsection—

(A) the term "production order" means an order to produce any tangible thing under this section; and

(B) the term "nondisclosure order" means an order imposed under subsection (d).

(2)

(A)

(i) A person receiving a production order may challenge the legality of that order by filing a petition with the pool established by section 1803 (e)(1) of this title. Not less than 1 year after the date of the issuance of the production order, the recipient of a production order may challenge the nondisclosure order imposed in connection with such production order by filing a petition to modify or set aside such nondisclosure order, consistent with the requirements of subparagraph (C), with the pool established by section 1803 (e)(1) of this title.

(ii) The presiding judge shall immediately assign a petition under clause (i) to 1 of the judges serving in the pool established by section 1803 (e)(1) of this title. Not later than 72 hours after the assignment of such petition, the assigned judge shall conduct an initial review of the petition. If the assigned judge determines that the petition is frivolous, the assigned judge shall immediately deny the petition and affirm the production order or

nondisclosure order. If the assigned judge determines the petition is not frivolous, the assigned judge shall promptly consider the petition in accordance with the procedures established under section 1803 (e)(2)of this title.

(iii) The assigned judge shall promptly provide a written statement for the record of the reasons for any determination under this subsection. Upon the request of the Government, any order setting aside a nondisclosure order shall be stayed pending review pursuant to paragraph (3).

(B) A judge considering a petition to modify or set aside a production order may grant such petition only if the judge finds that such order does not meet the requirements of this section or is otherwise unlawful. If the judge does not modify or set aside the production order, the judge shall immediately affirm such order, and order the recipient to comply therewith.

(C)

(i) A judge considering a petition to modify or set aside a nondisclosure order may grant such petition only if the judge finds that there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person.

(ii) If, upon filing of such a petition, the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director

of the Federal Bureau of Investigation certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations, such certification shall be treated as conclusive, unless the judge finds that the certification was made in bad faith.

(iii) If the judge denies a petition to modify or set aside a nondisclosure order, the recipient of such order shall be precluded for a period of 1 year from filing another such petition with respect to such nondisclosure order.

(D) Any production or nondisclosure order not explicitly modified or set aside consistent with this subsection shall remain in full effect.

(3) A petition for review of a decision under paragraph (2) to affirm, modify, or set aside an order by the Government or any person receiving such order shall be made to the court of review established under section 1803 (b) of this title, which shall have jurisdiction to consider such petitions. The court of review shall provide for the record a written statement of the reasons for its decision and, on petition by the Government or any person receiving such order for writ of certiorari, the record shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(4) Judicial proceedings under this subsection shall be concluded as expeditiously as possible. The record of proceedings, including petitions filed, orders granted, and statements of reasons for decision, shall be maintained under security measures established by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

(5) All petitions under this subsection shall be filed under seal. In any proceedings under this subsection, the court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions thereof, which may include classified information.

(g) Minimization procedures

(1) In general

Not later than 180 days after March 9, 2006, the Attorney General shall adopt specific minimization procedures governing the retention and dissemination by the Federal Bureau of Investigation of any tangible things, or information therein, received by the Federal Bureau of Investigation in response to an order under this subchapter.

(2) Defined

In this section, the term "minimization procedures" means—

(A) specific procedures that are reasonably designed in light of the purpose and technique of an order for the production of tangible things, to minimize the retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(B) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in section 1801 (e)(1) of this title, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand

foreign intelligence information or assess its importance; and

(C) notwithstanding subparagraphs (A) and (B), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.

(h) Use of information

Information acquired from tangible things received by the Federal Bureau of Investigation in response to an order under this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures adopted pursuant to subsection (g). No otherwise privileged information acquired from tangible things received by the Federal Bureau of Investigation in accordance with the provisions of this subchapter shall lose its privileged character. No information acquired from tangible things received by the Federal Bureau of Investigation in response to an order under this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes.

4. 15 U.S.C. 6501 provides in relevant part:

(8) Personal information

The term "personal information" means individually identifiable information about an individual collected online, including—

(A) a first and last name;

(B) a home or other physical address including street name and name of a city or town;

(C) an e-mail address;

(D) a telephone number;

(E) a Social Security number;

* * * * *

5. 18 U.S.C. 2725(3) provides:

(3) "personal information" means information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status.

6. 18 U.S.C. 3127(3) provides:

(3) the term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business * * *

7. 18 U.S.C. 3127(4) provides:

(4) the term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication * * *

8. 28 U.S.C. 1651 provides:

Writs

(a) The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.

(b) An alternative writ or rule nisi may be issued by a justice or judge of a court which has jurisdiction.

9. 47 U.S.C. 222(h) provides in relevant part:

Privacy of customer information

* * * * *

(h) Definitions

As used in this section:

(1) Customer proprietary network information

The term "customer proprietary network information" means—

(A) information that relates to the quantity, technical configuration, type, destination,

location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and

(B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier;

except that such term does not include subscriber list information.

* * * * *

10. 50 U.S.C. 1803 provides in relevant part:

Designation of judges

(a) Court to hear applications and grant orders; record of denial; transmittal to court of review

(1) The Chief Justice of the United States shall publicly designate 11 district court judges from at least seven of the United States judicial circuits of whom no fewer than 3 shall reside within 20 miles of the District of Columbia who shall constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this chapter, except that no judge designated under this subsection (except when sitting en banc under paragraph (2)) shall hear the same application for electronic surveillance under this chapter which has been denied previously by another judge designated under this subsection. If any judge so designated denies an application for an order authorizing electronic surveillance under this

chapter, such judge shall provide immediately for the record a written statement of each reason of his decision and, on motion of the United States, the record shall be transmitted, under seal, to the court of review established in subsection (b) of this section.

(2)

(A) The court established under this subsection may, on its own initiative, or upon the request of the Government in any proceeding or a party under section 1861 (f) of this title or paragraph (4) or (5) of section 1881a (h) of this title, hold a hearing or rehearing, en banc, when ordered by a majority of the judges that constitute such court upon a determination that—

(i) en banc consideration is necessary to secure or maintain uniformity of the court's decisions; or

(ii) the proceeding involves a question of exceptional importance.

(B) Any authority granted by this chapter to a judge of the court established under this subsection may be exercised by the court en banc. When exercising such authority, the court en banc shall comply with any requirements of this chapter on the exercise of such authority.

(C) For purposes of this paragraph, the court en banc shall consist of all judges who constitute the court established under this subsection.

(b) Court of review; record, transmittal to Supreme Court

The Chief Justice shall publicly designate three judges, one of whom shall be publicly designated as the presiding judge, from the United States district courts or courts of appeals who together shall

comprise a court of review which shall have jurisdiction to review the denial of any application made under this chapter. If such court determines that the application was properly denied, the court shall immediately provide for the record a written statement of each reason for its decision and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

11. 50 U.S.C. 1841 provides:

Definitions

As used in this subchapter:

(1) The terms "foreign power", "agent of a foreign power", "international terrorism", "foreign intelligence information", "Attorney General", "United States person", "United States", "person", and "State" shall have the same meanings as in section 1801 of this title.

(2) The terms "pen register" and "trap and trace device" have the meanings given such terms in section 3127 of title 18.

(3) The term "aggrieved person" means any person—

(A) whose telephone line was subject to the installation or use of a pen register or trap and trace device authorized by this subchapter; or

(B) whose communication instrument or device was subject to the use of a pen register or trap and trace device authorized by this subchapter to capture incoming electronic or other communications impulses.

12. 50 U.S.C. 1842 provides:

Pen registers and trap and trace devices for foreign intelligence and international terrorism investigations

(a) Application for authorization or approval

(1) Notwithstanding any other provision of law, the Attorney General or a designated attorney for the Government may make an application for an order or an extension of an order authorizing or approving the installation and use of a pen register or trap and trace device for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution which is being conducted by the Federal Bureau of Investigation under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order.

(2) The authority under paragraph (1) is in addition to the authority under subchapter I of this chapter to conduct the electronic surveillance referred to in that paragraph.

(b) Form of application; recipient

Each application under this section shall be in writing under oath or affirmation to—

(1) a judge of the court established by section 1803 (a) of this title; or

(2) a United States Magistrate Judge under chapter 43 of title 28 who is publicly designated by

the Chief Justice of the United States to have the power to hear applications for and grant orders approving the installation and use of a pen register or trap and trace device on behalf of a judge of that court.

(c) Executive approval; contents of application

Each application under this section shall require the approval of the Attorney General, or a designated attorney for the Government, and shall include—

(1) the identity of the Federal officer seeking to use the pen register or trap and trace device covered by the application; and

(2) a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

(d) Ex parte judicial order of approval

(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the installation and use of a pen register or trap and trace device if the judge finds that the application satisfies the requirements of this section.

(2) An order issued under this section—

(A) shall specify—

(i) the identity, if known, of the person who is the subject of the investigation;

(ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied; and

(iii) the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order;

(B) shall direct that—

(i) upon request of the applicant, the provider of a wire or electronic communication service, landlord, custodian, or other person shall furnish any information, facilities, or technical assistance necessary to accomplish the installation and operation of the pen register or trap and trace device in such a manner as will protect its secrecy and produce a minimum amount of interference with the services that such provider, landlord, custodian, or other person is providing the person concerned;

(ii) such provider, landlord, custodian, or other person—

(I) shall not disclose the existence of the investigation or of the pen register or trap and trace device to any person unless or until ordered by the court; and

(II) shall maintain, under security procedures approved by the Attorney

General and the Director of National Intelligence pursuant to section 1805 (b)(2)(C) of this title, any records concerning the pen register or trap and trace device or the aid furnished; and

(iii) the applicant shall compensate such provider, landlord, custodian, or other person for reasonable expenses incurred by such provider, landlord, custodian, or other person in providing such information, facilities, or technical assistance; and

(C) shall direct that, upon the request of the applicant, the provider of a wire or electronic communication service shall disclose to the Federal officer using the pen register or trap and trace device covered by the order—

(i) in the case of the customer or subscriber using the service covered by the order (for the period specified by the order)—

(I) the name of the customer or subscriber;

(II) the address of the customer or subscriber;

(III) the telephone or instrument number, or other subscriber number or identifier, of the customer or subscriber, including any temporarily assigned network address or associated routing or transmission information;

(IV) the length of the provision of service by such provider to the customer or subscriber and the types of services utilized by the customer or subscriber;

(V) in the case of a provider of local or long distance telephone service, any local or long distance telephone records of the customer or subscriber;

(VI) if applicable, any records reflecting period of usage (or sessions) by the customer or subscriber; and

(VII) any mechanisms and sources of payment for such service, including the number of any credit card or bank account utilized for payment for such service; and

(ii) if available, with respect to any customer or subscriber of incoming or outgoing communications to or from the service covered by the order—

(I) the name of such customer or subscriber;

(II) the address of such customer or subscriber;

(III) the telephone or instrument number, or other subscriber number or identifier, of such customer or subscriber, including any temporarily assigned network address or associated routing or transmission information; and

(IV) the length of the provision of service by such provider to such customer or subscriber and the types of services utilized by such customer or subscriber.

(e) Time limitation

(1) Except as provided in paragraph (2), an order issued under this section shall authorize the installation and use of a pen register or trap and

trace device for a period not to exceed 90 days. Extensions of such an order may be granted, but only upon an application for an order under this section and upon the judicial finding required by subsection (d) of this section. The period of extension shall be for a period not to exceed 90 days.

(2) In the case of an application under subsection (c) where the applicant has certified that the information likely to be obtained is foreign intelligence information not concerning a United States person, an order, or an extension of an order, under this section may be for a period not to exceed one year.

(f) Cause of action barred

No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance under subsection (d) of this section in accordance with the terms of an order issued under this section.

(g) Furnishing of results

Unless otherwise ordered by the judge, the results of a pen register or trap and trace device shall be furnished at reasonable intervals during regular business hours for the duration of the order to the authorized Government official or officials.

13. The Judiciary Act of 1789 provides in relevant part:

Sec. 21: *And be it further enacted*, That from final decrees in a district court in causes of admirality and maritime jurisdiction, where the matter in dispute

exceeds the sum or value of three hundred dollars, exclusive of costs, an appeal shall be allowed to the next circuit court, to be held in such district. Provided nevertheless, That all such appeals from final decrees as aforesaid, from the district court of Maine, shall be made to the circuit court, next to be holden after each appeal in the district of Massachusetts.

Sec. 22: *And be it further enacted*, That final decrees and judgments in civil actions in a district court, where the matter in dispute exceeds the sum or value of fifty dollars, exclusive of costs, may be reexamined, and reversed or affirmed in a circuit court, holden in the same district, upon a writ of error, whereto shall be annexed and returned therewith at the day and place therein mentioned, an authenticated transcript of the record, an assignment of errors, and prayer for reversal, with a citation to the adverse party, signed by the judge of such district court, or a justice of the Supreme Court, the adverse party having at least twenty days' notice. And upon a like process, may final judgments and decrees in civil actions, and suits in equity in a circuit court, brought there by original process, or removed there from courts of the several States, or removed there by appeal from a district court where the matter in dispute exceeds the sum or value of two thousand dollars, exclusive of costs, be re-examined and reversed or affirmed in the Supreme Court, the citation being in such case signed by a judge of such circuit court, or justice of the Supreme Court, and the adverse party having at least thirty days' notice. But there shall be no reversal in either court on such writ of error for error in ruling any plea in abatement, other than a plea to the jurisdiction of the court, or

such plea to a petition or bill in equity, as is in the nature of a demurrer, or for any error in fact. And writs of error shall not be brought but within five years after rendering or passing the judgment or decree complained of, or in case the person entitled to such writ of error be an infant, feme covert, non compos mentis, or imprisoned, then within five years as aforesaid, exclusive of the time of such disability. And every justice or judge signing a citation on any writ of error as aforesaid, shall take good and sufficient security, that the plaintiff in error shall prosecute his writ to effect, and answer all damages and costs if he fail to make his plea good.

* * * * *

Sec. 25: *And be it further enacted*, That a final judgment or decree in any suit, in the highest court of law or equity of a State in which a decision in the suit could be had, where is drawn in question the validity of a treaty or statute of, or an authority exercised under the United States, and the decision is against their validity; or where is drawn in question the validity of a statute of, or an authority exercised under any State, on the ground of their being repugnant to the constitution, treaties or laws of the United States, and the decision is in favour of such their validity, or where is drawn in question the construction of any clause of the constitution, or of a treaty, or statute of, or commission held under the United States, and the decision is against the title, right, privilege or exemption specially set up or claimed by either party, under such clause of the said Constitution, treaty, statute or commission, may be re-examined and reversed or affirmed in the Supreme Court of the United States upon a writ of error, the citation being signed by the chief justice, or judge or

chancellor of the court rendering or passing the judgment or decree complained of, or by a justice of the Supreme Court of the United States, in the same manner and under the same regulations, and the writ shall have the same effect, as if the judgment or decree complained of had been rendered or passed in a circuit court, and the proceeding upon the reversal shall also be the same, except that the Supreme Court, instead of remanding the cause for a final decision as before provided, may at their discretion, if the cause shall have been once remanded before, proceed to a final decision of the same, and award execution. But no other error shall be assigned or regarded as a ground of reversal in any such case as aforesaid, than such as appears on the face of the record, and immediately respects the before mentioned questions of validity or construction of the said constitution, treaties, statutes, commissions, or authorities in dispute.

14. 47 C.F.R. § 64.2003 provides in relevant part:

§ 64.2003 Definitions.

(d) Call detail information. Any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.

15. Exec. Order No. 12,333, 46 Fed. Reg. 59941 (1981), *as amended by* Exec. Order No. 13,284, 68 Fed. Reg. 4075 (2003), Exec. Order No. 13,355, 69 Fed. Reg. 53,593 (2004), and Exec. Order No. 13,470,

73 Fed. Reg. 45,325 (2008), provides in relevant parts:

§ 1.1 *Goals*

(b) The United States Government has a solemn obligation, and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law.

§ 1.7 *Intelligence Community Elements*

(c) THE NATIONAL SECURITY AGENCY. The Director of the National Security Agency shall:

(1) Collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;

§ 2.3 *Collection of Information*

(b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the Federal Bureau of Investigation (FBI) or, when significant foreign intelligence is sought, by other authorized elements of the Intelligence Community, provided that no foreign intelligence collection by such elements may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;

§ 2.4 *Collection Techniques*

Elements of the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Elements of the Intelligence Community are not authorized to use such techniques as electronic surveillance, unconsented physical searches, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element and approved by the Attorney General, after consultation with the Director. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes. . . .

16. Foreign Intelligence Surveillance Ct. R.33(a) provides in relevant part:

Petition Challenging Production or Nondisclosure Order.

(a) Who May File. The recipient of a production order or nondisclosure order under 50 U.S.C. § 1861 ("petitioner") may file a petition challenging the order pursuant to 50 U.S.C. § 1861(f). A petition may be filed by the petitioner's counsel.

17. Foreign Intelligence Surveillance Ct. R.46 provides:

Initial Hearing En Banc on Request of a Party. The government in any proceeding, or a party in a

proceeding under 50 U.S.C. § 1861(f) or 50 U.S.C. § 1881a(h)(4)-(5), may request that the matter be entertained from the outset by the full Court. However, initial hearings en banc are extraordinary and will be ordered only when a majority of the Judges determines that a matter is of such immediate and extraordinary importance that initial consideration by the en banc Court is necessary, and en banc review is feasible in light of applicable time constraints on Court action.

18. Sup. Ct. R. 20.1 provides in relevant part:

Procedure On A Petition For An Extraordinary Writ

1. Issuance by the Court of an extraordinary writ authorized by 28 U. S. C. §1651(a) is not a matter of right, but of discretion sparingly exercised. To justify the granting of any such writ, the petition must show that the writ will be in aid of the Court's appellate jurisdiction, that exceptional circumstances warrant the exercise of the Court's discretionary powers, and that adequate relief cannot be obtained in any other form or from any other court.