No. 13-58

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

BRIEF OF *AMICUS CURIAE* PROFESSORS OF INFORMATION PRIVACY AND SURVEILLANCE LAW IN SUPPORT OF PETITIONER

FRED H. CATE
Counsel of Record
INDIANA UNIVERSITY
MAURER SCHOOL OF LAW
211 S. Indiana Avenue
Bloomington, IN 47405
(812) 855-1161
fcate@indiana.edu

August 9, 2013

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES iii

INTEREST OF AMICUS CURIAE 1

SUMMARY OF ARGUMENT..... 3

ARGUMENT 4

I. Background 4

A. The Verizon Order..... 4

B. The Foreign Intelligence Surveillance Act..... 6

II. The Verizon Order Fails to Meet the Requirements of Section 215..... 9

A. Call Detail Records and Telephony Metadata on all Domestic Verizon Calls Could Not be "Relevant to an Authorized Investigation," as Required by Section 215... 10

1. "Reasonable Grounds"..... 11

2. "Relevant" 11

3. "Authorized Investigation" 13

4. The Government Acknowledges that Most of the Data Collected Under the Verizon Order is Not "Relevant" 15

5. The "Primary Order" Does Not Affect the Determination of Relevance 17

6. The Government's Defense of the Verizon Order Ignores the Language and History of Section 215 18

B. The Verizon Order is Contrary to Executive Order 12333 and the *Attorney General's Guidelines* 22

C. The Investigation is Being Conducted "Solely Upon the Basis of Activities Protected by the First Amendment to the Constitution" in Violation of Section 215 24

CONCLUSION 26

TABLE OF AUTHORITIES

Page

CASES

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 (RV) (FISA Ct. Apr. 25, 2013) 3-5, 10

In re Application of the FBI for an Order Requiring the Production of Tangible Things from [redacted], Dkt. No. BR [redacted] (RV) (FISA Ct. Apr. 25, 2013) 17

Park 'N Fly, Inc. v. Dollar Park & Fly, Inc., 469 U.S. 189 (1985)..... 10

Reiter v. Sonotone Corp., 442 U.S. 330 (1979) 19

Sable Communications of Calif. v. FCC, 492 U.S. 115 (1989) 25

Terry v. Ohio, 392 U.S. 1 (1968) 11-12

United States v. Jones, 132 S. Ct. 945 (2012) 26

United States v. United States District Court, 407 U.S. 297 (1972) 20-21, 26

CONSTITUTIONAL PROVISIONS

U.S. CONST. amend. I 10

STATUTES

50 U.S.C. 1861 ..... 8-11, 14, 18-19, 23-25, 27

Foreign Intelligence Surveillance Act of 1978, Pub. L. 95-511, Oct. 25, 1978 6

Intelligence Authorization Act for Fiscal Year 1999, Pub. L. 105-272, Oct. 20, 1998 6

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107-56, Oct. 26, 2001 7

USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109-177, Mar. 9, 2006... 7, 22

LEGISLATIVE MATERIALS

151 CONG. REC. S9559 (July 29, 2005) 12

151 CONG. REC. S9561 (July 29, 2005) 12

Oversight of the Administration's use of FISA Authorities Before the H. Comm. on the Judiciary, 113th Cong. (July 17, 2013)..... 12, 20

Oversight of FISA Surveillance Programs Before the S. Comm. on the Judiciary, 113th Cong. (July 31, 2013)..... 17-18

S. REP. NO. 95-604(I), at 7 (1977), *as reprinted* in 1978 U.S.C.C.A.N. 3904, 3908..... 6

MISCELLANEOUS

47 C.F.R. § 64.2003 (2012) 5

DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS (2d. ed. 2012)..... 10, 20

Exec. Order No. 12333, 46 Fed. Reg. 59941 (Dec. 4, 1981) 23-24, 27

Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, GUARDIAN, June 5, 2013 5

Letter from DNI James Clapper to Senator Ron Wyden, July 2013..... 5

Letter from Twenty Six Senators to the Honorable James Clapper, June 27, 2013 25

Letter from Peter J. Kadzik, Principal Deputy Assistant Attorney General, to Representative James Sensenbrenner, July 16, 2013 16

MARSHALL CURTIS ERWIN & EDWARD C. LIU, CONG. RESEARCH SERV., R4314, NSA SURVEILLANCE LEAKS: BACKGROUND AND ISSUES FOR CONGRESS (2013)..... 5, 10

Merriam-Webster's Collegiate Dictionary, "Relevant," 1051 (11th ed. 2004) 12

Office of the DNI, *DNI Statement on Recent Unauthorized Disclosures of Classified Information*, June 6, 2013 15

Office of the DNI, *Foreign Intelligence Surveillance Court Renews Authority to Collect Telephony Metadata,* July 19, 2013 6

Office of the DNI, *Newseum Special Program—NSA Surveillance Leaks: Facts and Fiction*, June 26, 2013 ..... 15-16, 19-20, 22

Rep. Jim Sensenbrenner, *This Abuse of the Patriot Act Must End*, GUARDIAN, June 9, 2013..... 17

Ronald D. Lee & Paul M. Schwartz, *Beyond the "War" on Terrorism: Towards the New Intelligence Network*, 103 MICH. L. REV. 1446 (2005)..... 21

TECH. AND PRIVACY ADVISORY COMM., U.S. DEP'T OF DEF., SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM (2004) 21-22, 27

U.S. DEP'T OF DEFENSE, TAPAC RECOMMENDATION WITH IOB RECOMMENDATIONS (Aug. 15, 2006) .. 22

U.S. DEP'T OF JUSTICE, ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS (2008) 13, 23-26

VERIZON COMMUNICATIONS, FACT SHEET (Dec. 31, 2012) 10

VERIZON COMMUNICATIONS, CORPORATE OVERVIEW (Apr. 29, 2013) 10

INTEREST OF *AMICUS CURIAE*[1]

Amici are professors with broad experience in the history, application, and impact of information privacy and surveillance law and the legal provision on which the challenged order is based, and a professional interest in its rational interpretation. *Amici* are (institutions are listed for identification purposes only):

William C. Banks
Board of Advisors Distinguished Professor
Syracuse University College of Law
Director, Institute for National Security and Counterterrorism

Fred H. Cate (Counsel of Record)
Distinguished Professor and C. Ben Dutton Professor of Law
Indiana University Maurer School of Law
Director, Center for Applied Cybersecurity Research

Danielle Citron
Lois K. Macht Research Professor of Law
University of Maryland
Francis King Carey School of Law

David P. Fidler
James Louis Calamaras Professor of Law
Indiana University Maurer School of Law

---

[1]No counsel for any party authored this brief in whole or in part. No other persons other than the *amicus curiae* have made a monetary contribution to its preparation or submission. The parties have consented to the filing of this brief, and communications reflecting that consent are submitted to the Clerk's office with this brief.

Susan Freiwald
Professor of Law
University of San Francisco School of Law

Lawrence M. Friedman
Professor of Law
New England Law—Boston

Michael Froomkin
Laurie Silvers & Mitchell Rubenstein
Distinguished Professor of Law
University of Miami School of Law

Ken Gormley
Dean and Professor of Law
Duquesne University School of Law

Deirdre Mulligan
Assistant Professor
University of California Berkeley
School of Information

Paul Ohm
Associate Professor of Law
University of Colorado Law School

Joel R. Reidenberg
Stanley D. and Nikki Waxberg Chair and
Professor of Law
Founding Academic Director, Center on Law
and Information Policy
Fordham University School of Law

Ira S. Rubinstein
Senior Fellow and Adjunct Professor
New York University School of Law

Peter Swire
C. William O'Neill Professor in Law and
Judicial Administration
Ohio State University Moritz College of Law

Jennifer M. Urban
Assistant Clinical Professor of Law
University of California, Berkeley
School of Law
Director, Samuelson Law, Technology & Public
Policy Clinic

SUMMARY OF ARGUMENT

On April 25, 2013, the Foreign Intelligence Surveillance Court ("FISC"), issued an order under 50 U.S.C. § 1861 compelling Verizon Business Network Services, Inc. ("Verizon") to produce to the National Security Agency ("NSA") on a daily basis an electronic copy of "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. . ." *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 (RV) at 1-2 (FISA Ct. Apr. 25, 2013) ("Verizon Order").

The order violates the language and logic of 50 U.S.C. § 1861 by permitting the federal government to engage in the unlawful wholesale collection of personal information about "U.S. persons" (i.e., U.S. citizens and permanent legal residents). The government's defense of the Verizon Order reflects a significant rewriting of the law and permits the illegal

construction of a comprehensive database of data about U.S. persons' communications. The Verizon Order thus warrants the extraordinary remedy of mandamus because it clearly violates the law and presents an extraordinary risk to personal privacy.

As scholars of U.S. information privacy and surveillance law, we respectfully urge the Court to grant the writ of mandamus and to vacate the order and prohibit such future orders from the FISC, or, in the alternative, to grant the writ of certiorari to review the Verizon Order.

ARGUMENT

I. Background

A. The Verizon Order

On April 25, 2013, the Honorable Roger Vinson of the FISC issued an order under 50 U.S.C. § 1861 compelling Verizon to produce to the NSA on a daily basis an electronic copy of "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. . ." Verizon Order at 1-2. The only calls excluded from the Verizon Order are "communications wholly originating and terminating in foreign countries." *Id.* at 2.

The order defines "telephony metadata" to include:

> 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.

Id. The order does not define "call detail records," but the Federal Communications Commission defines the term to mean: "[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).

Although the order was classified, it was published in *The Guardian* on June 5, 2013. Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, GUARDIAN, June 5, 2013. "Intelligence officials and leaders of the congressional intelligence committees have confirmed the existence of this domestic phone records collection program . . . ." MARSHALL CURTIS ERWIN & EDWARD C. LIU, CONG. RESEARCH SERV., R4314, NSA SURVEILLANCE LEAKS: BACKGROUND AND ISSUES FOR CONGRESS (2013).

The Director of National Intelligence ("DNI") has confirmed that the Verizon order is part of an ongoing electronic surveillance program that began in May 2006 and has been reauthorized by the FISC approximately every 90 days since. *See* Letter from DNI James Clapper to Senator Ron Wyden, July 2013, at 2. The Verizon Order was set to expire on

July 19, 2013. Verizon Order at 4. The Office of the DNI has confirmed that the FISC has again renewed the order. *See* Office of the DNI, *Foreign Intelligence Surveillance Court Renews Authority to Collect Telephony Metadata,* July 19, 2013.

B. The Foreign Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. 95-511, Oct. 25, 1978, created the court issuing the Verizon order and the authority under which the order was issued. FISA, as amended, does not grant the FISC the power to authorize the wholesale collection of call detail records and telephony metadata about U.S. persons.

Congress enacted FISA to prevent "warrantless electronic surveillance" of U.S. persons by government intelligence agencies "in the name of national security," S. REP. NO. 95-604(I), at 7 (1977), *as reprinted* in 1978 U.S.C.C.A.N. 3904, 3908, and it created the FISC to oversee and authorize such surveillance. *Id.*

In 1998, Congress amended FISA to authorize the production of certain business records about those suspected of being foreign powers or agents of a foreign power. *See* Intelligence Authorization Act for Fiscal Year 1999, Pub. L. 105-272, Oct. 20, 1998, § 602. Under the 1998 statute, records could be sought from: (1) common carriers, (2) public accommodation facilities, (3) storage facilities, and (4) vehicle rental facilities. *Id.*

Shortly after the terrorist attacks of September 11, 2001, Congress adopted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism

Act of 2001 ("USA PATRIOT Act"). Pub. L. 107-56, Oct. 26, 2001. Section 215 of the USA PATRIOT Act expanded the range of material the government could obtain. § 215.

Section 215 authorized intelligence agencies to apply for an order from the FISC "requiring the production of any tangible things (including books, records, papers, documents, and other items)." *Id.* Congress required that the records be "sought for an authorized investigation;" that the investigation "be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order);" and that, when directed towards a U.S. person, the investigation not be "conducted solely upon the basis of activities protected by the first amendment to the Constitution." § 215(a)(2). Congress specified that § 215 would sunset on December 31, 2005. § 224.

In 2006, Congress revised § 215 to heighten the government's burden in obtaining a FISA order. *See* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109-177, Mar. 9, 2006. Instead of showing that data were "sought for" an investigation, the 2006 amendments require the government to submit a statement of facts establishing "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." § 106.

Congress also added a provision requiring that an investigation "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," *id*., reinforcing similar language that was already in the law. *See* 50 U.S.C. § 1861(a)(1). Congress directed applicants to provide "an enumeration of the minimization procedures adopted by the Attorney General . . . that are applicable to the retention and dissemination" of anything obtained under 50 U.S.C. § 1861. *Id.*

Thus, the law under which the FISC granted the Verizon Order authorizes the Federal Bureau of Investigation ("FBI"), on its own behalf or on behalf of another intelligence agency, to apply for a FISC order to compel the production of "tangible things." 50 U.S.C. § 1861(a)(1). For the application to be valid, four requirements must be met:

1. 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 (other than a threat assessment). . . ." § 1861(b)(2)(A).

2. The investigation must "be conducted under guidelines approved by the Attorney General under Executive Order 12333." § 1861(a)(2)(A).

3. When directed toward a U.S. person, the investigation must not be conducted "solely upon the basis of activities protected by the first amendment to the Constitution." §§ 1861(a)(1), (a)(2)(B).

4. The application must contain "an enumeration of the minimization procedures adopted by the Attorney General . . . that are applicable to the

retention and dissemination" of any tangible things obtained under § 1861. § 1861(b)(2)(B).

If the FISC finds that the application meets the statutory requirements, the FISC "shall enter an ex parte order as requested, or as modified, approving the release of tangible things." § 1861(c)(1).

II. The Verizon Order Fails to Meet the Requirements of Section 215

The Verizon Order fails to meet the requirements of § 215.[2] *See* 50 U.S.C. § 1861. Specifically, it is not limited to call detail records and telephony metadata about which there are "reasonable grounds" to believe the data are "relevant to an authorized investigation (other than a threat assessment)." § 1861(b)(2)(A). The government acknowledges that the vast majority of data collected under the Verizon Order has not been relevant to any investigation, and its argument that the NSA can assess relevance on its own after the data are collected violates the plain language of § 215. *See infra* II.A.4-6.

In addition, the Verizon Order is inconsistent with Executive Order 12333 and the guidelines adopted thereunder, and it authorizes the collection of call detail records and telephony metadata U.S. persons generate solely by activities protected by the First Amendment to the U.S. Constitution, in

---

[2] This brief addresses only the statutory issues raised by the order under 50 U.S.C. § 1861; it does not address the constitutional issues raised by the Verizon Order.

violation of § 215. *See* 50 U.S.C. §§ 1861(a)(1), 1861(a)(2)(B); U.S. CONST. amend. I.

A. Call Detail Records and Telephony Metadata on all Domestic Verizon Calls Could Not be "Relevant to an Authorized Investigation"

This Court has stressed that "[s]tatutory construction must begin with the language employed by Congress and the assumption that the ordinary meaning of that language accurately expresses the legislative purpose." *Park 'N Fly, Inc. v. Dollar Park & Fly, Inc.*, 469 U.S. 189, 194 (1985).

It is inconceivable that call detail records and telephony metadata on all domestic Verizon calls could be "relevant to an authorized investigation," as required by section 215. § 1861(b)(2)(A).

Verizon is the United States' largest wireless service provider, with 98.9 million wireless retail customers. VERIZON COMMUNICATIONS, FACT SHEET (Dec. 31, 2012). It also operates the nation's largest all fiber network, which carries an average of 1 billion residential and small business calls a day. *Id.*; *see also* VERIZON COMMUNICATIONS, CORPORATE OVERVIEW (Apr. 29, 2013).

For the FISC to have found that the FBI's application "satisfies the requirements of 50 U.S.C. § 1861," Verizon Order at 1, the court would have had to conclude that the FBI had "reasonable grounds" to believe that the call detail records and telephony metadata concerning the billions of calls by or to millions of customers were "relevant to an authorized investigation." § 1861(b)(2)(A). This is not credible. It is not possible that the government could be

conducting an "authorized investigation" of all of Verizon's millions of customers or that the FBI had "reasonable grounds" to believe that call detail records and telephony metadata from all, or even a significant portion, of Verizon's billions of calls were relevant to an authorized investigation.

FISA does not define "reasonable grounds," "relevant," and "authorized" investigation, therefore other sources for the meaning of each are considered below.

1. "Reasonable Grounds"

According to David S. Kris, former United States Assistant Attorney General for National Security, and J. Douglas Wilson, Chief of the Criminal Division and former Chief of the National Security Unit in the U.S. Attorney's Office for the Northern District of California, courts often use the terms "reasonable grounds" and "reasonable suspicion" interchangeably. DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS §§ 2.2-2.6, 3.4 (2d. ed. 2012); *see also* ERWIN & LIU, *supra* at 4-5.

When applying a "reasonable grounds" standard, this Court has required a showing of some form 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).

2. "Relevant"

FISA also does not define what makes a tangible thing "relevant" to an authorized investigation. *Merriam-Webster's Collegiate*

Dictionary defines "relevant" to mean "having significant and demonstrable bearing on the matter at hand" or "affording evidence tending to prove or disprove the matter at issue or under discussion . . . . " *Merriam-Webster's Collegiate Dictionary*, "Relevant," 1051 (11th ed. 2004).

During a House Judiciary Committee hearing on July 17, 2013, the author of § 215, Representative James Sensenbrenner (R-WI) stated that Congress revised the statute in 2006 to impose the relevancy requirement in "an attempt to limit what the intelligence community could be able to get pursuant to Section 215." *Oversight of the Administration's use of FISA Authorities Before the H. Comm. on the Judiciary,* 113th Cong. (July 17, 2013) (comments of Rep. James Sensenbrenner).

Statements by legislators made during the debate over the 2006 amendments express similar sentiments. *See, e.g.*, 151 CONG. REC. S9559 (July 29, 2005) (statement of Sen. Ron Wyden) (section 215's relevance standard "addresses concerns about government 'fishing' expeditions"); 151 CONG. REC. S9561 (July 29, 2005) (statement of Sen. Patrick Leahy) (amendments to § 215 protect "the civil liberties of Americans . . . . by requiring that a judge determine that the request is relevant to a national security intelligence investigation").

3. "Authorized Investigation"

The *Attorney General's Guidelines for FBI Domestic Operations* authorize three levels of investigations: assessments, preliminary investigations, and full investigations. *See* U.S. DEP'T OF JUSTICE, ATTORNEY GENERAL'S GUIDELINES FOR

DOMESTIC FBI OPERATIONS 17-18 (2008) ("ATTORNEY GENERAL'S GUIDELINES"). FISA expressly bars threat assessments from forming the basis for a FISA order application. 50 U.S.C. § 1861(b)(2)(A).

The *Attorney General's Guidelines* describe preliminary and full investigations as "predicated investigations," meaning that they must be predicated on "allegations, reports, facts or circumstances indicative of possible criminal or national security-threatening activity, or the potential for acquiring information responsive to foreign intelligence requirements . . . . " ATTORNEY GENERAL'S GUIDELINES at 18.

Initiating preliminary investigations requires an "allegation or information indicative of possible criminal or national security-threatening activity." *Id.* Full investigations require "an articulable factual basis for the investigation that reasonably indicates" the existence of some activity constituting a federal crime, a threat to national security, or foreign intelligence. *Id.* In contrast, assessments—which § 215 does not permit as a basis for gathering U.S. persons' communications—do not require any factual predicate. *Id.*

By requiring that a "statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation" must support the application for an order under 50 U.S.C. § 1861, and that the authorized investigation must be something "other than a threat assessment," Congress clearly intended that some factual predicate undergird the investigation and that

the "tangible things" sought be relevant to that predicate. § 1861(b)(2)(A).

The government does not and could not have a factual predicate to investigate all of Verizon's more than 98.9 million customers. Nor is it possible that the government is conducting an authorized investigation of such scope that all, or even most, call detail records or telephony metadata from the hundreds of billions of calls handled by Verizon each year would be relevant.

To the extent the FISC construed "authorized investigation" to include broad government efforts to combat terrorism generally, nothing in FISA supports this reading. Quite the contrary, the fact that Congress specifically excluded "threat assessment" from the universe of "authorized investigations" sufficient to justify an order from the FISC under § 215 indicates that Congress rejected such a broad claim. Moreover, because the vast majority of U.S. persons are not involved in terrorist activity, the government has no "reasonable grounds" to consider their communications "relevant" to such an investigation—which the government, as described below, concedes.

4. The Government Acknowledges that Most of the Data Collected Under the Verizon Order is Not "Relevant"

The government has acknowledged that the vast majority of data it has obtained under the Verizon Order is not "relevant to an authorized investigation." The DNI's office issued a statement on June 6, 2013, that the NSA is collecting data under the Verizon Order only so that those data later may

be "queried when there is a reasonable suspicion, based on specific facts, that the particular basis for the query is associated with a foreign terrorist organization." Office of the DNI, *DNI Statement on Recent Unauthorized Disclosures of Classified Information*, June 6, 2013.

Robert Litt, General Counsel to the DNI, described the government's access to the data collected under the Verizon Order in nearly identical terms on June 25, 2013: "The metadata that is acquired and kept under this program can only be queried when there is reasonable suspicion, based on specific, articulable facts, that a particular telephone number is associated with specified foreign terrorist organizations." Office of the DNI, *Newseum Special Program—NSA Surveillance Leaks: Facts and Fiction*, June 26, 2013 (statement of Robert Litt).

Mr. Litt went on to say that "only a small portion of the data that is collected is ever actually reviewed, because the *vast majority of that data is never going to be responsive* to one of these terrorism-related queries." *Id.* (emphasis added). In fact, he reported that in 2012, "fewer than 300 identifiers were approved for searching this data." *Id.*

Rather than limit the Verizon Order, as FISA requires, to collecting only the call detail records and telephony metadata for which there were "reasonable grounds to believe [the records] are relevant to an authorized investigation," the NSA instead sought, and continues to get, vastly more data, the majority of which, according to the DNI's General Counsel, are "never going to be responsive to one of these terrorism-related queries." *Id*. In Mr. Litt's words: "we

collect all the data because if you want to find a needle in the haystack, you need to have the haystack." *Id.*

The DOJ reaffirmed this position on July 16, 2013:

> the FISC allows the data to be queried for intelligence purposes only when there is a reasonable suspicion, based on specific facts, that a particular query term, such as a telephone number is associated with a specific foreign terrorist organization that was previously identified to and approved by the court.

Letter from Peter J. Kadzik, Principal Deputy Assistant Attorney General, to Representative James Sensenbrenner, July 16, 2013.

The standard that the Principal Deputy Assistant Attorney General applies to data *after* collection, is in fact the standard required by § 215 *before* the data are collected in the first place. His letter fails to recognize this problem, and confirms that hundreds of billions of records gathered were entirely unrelated to objects of the government's interest, and so failed to meet the statutory standard: "NSA has reported that in 2012, fewer than 300 unique identifiers were used to query the data after meeting this standard." *Id.*

Representative Sensenbrenner writes that Congress never intended or understood § 215 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*, GUARDIAN, June 9, 2013.

5. The "Primary Order" Does Not Affect the Determination of Relevance

On July 31, 2013, the DNI released a declassified version of another FISC order, which the DNI refers to as the "primary order." *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [redacted],* Dkt. No. BR [redacted] (RV) (FISA Ct. Apr. 25, 2013) ("Primary Order"); *Oversight of FISA Surveillance Programs Before the S. Comm. on the Judiciary*, 113th Cong. (July 31, 2013) (statement of Deputy Attorney General James Cole).

Government officials have argued that the Primary Order is necessary to understanding the lawfulness of the Verizon Order. DNI General Counsel Litt testified before the Senate Judiciary Committee that

> [y]ou have to look at [the Verizon Order] in the context of the primary order, which was declassified and issued today, that says the only way you can access [data already collected] is if you have reasonable, articulable suspicion that the number you are going to query off of is in fact related to specific terrorist groups.

Oversight of FISA Surveillance Programs (statement of Robert Litt).

The Primary Order, which established the requirements under which NSA officials may access data already collected under FISC surveillance orders, has no bearing on whether the FISC properly determined that there were "reasonable grounds" to believe that the call detail records and telephony metadata the government collected under the Verizon Order were "relevant to an authorized investigation (other than a threat assessment)." 50 U.S.C. § 1861(b)(2)(A). The protections in place for data *after* collection are not relevant to whether the statutory requirement for assessing relevancy *before* collection was met. In the case of the Verizon Order, it is clear the relevancy requirement of § 215 was not met.

6. The Government's Defense of the Verizon Order Ignores the Language and History of Section 215

Prior to passage of FISA, no statutory law restricted the NSA from conducting broad dragnet sweeps of data about U.S. persons. Congress enacted FISA to interpose a court between the NSA and such data. Over time, Congress amended FISA to broaden the range of things the government might access, but also imposed increasingly restrictive conditions under which the FISC could permit such access. The current statutory language reflects this tradeoff: the government may broadly access "tangible things," but to do so it must provide 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)." 50 U.S.C. § 1861(b)(2)(A).

This Court has stated that "[i]n construing a statute we are obliged to give effect, if possible, to every word Congress used." *Reiter v. Sonotone Corp.*, 442 U.S. 330, 339 (1979). The DNI's and DOJ's arguments effectively eliminate the word "relevant" from § 215 in two ways. First, they apply the relevancy requirement only after data are collected, not before collection. As the DNI's General Counsel said, first the call detail records and telephony metadata are "acquired and kept under this program." *NSA Surveillance Leaks: Facts and Fiction* (statement of Robert Litt). Then, later, the tiny amount of data within this comprehensive database that meets the statutory standard of relevance may be retrieved "when there is reasonable suspicion, based on specific, articulable facts, that a particular telephone number is associated with specified foreign terrorist organizations." *Id.*

Alternatively, the government makes the extraordinary claim that *all* call detail records and telephony metadata from Verizon are relevant under § 215 because somewhere within that vast dataset there may be individual data elements that are, in fact, relevant. The government argues that the FISC can authorize the collection of data from hundreds of billions of Verizon calls, even though "only a small portion of the data that is collected is ever actually reviewed, because the vast majority of that data is never going to be responsive to one of these terrorism-related queries." *Id.*

If a larger dataset is relevant because any element within it is relevant, then a dataset of all data must be relevant because somewhere within all the data relevant information is "reasonably likely" to

be found. This argument renders the word "relevant" in § 215 meaningless, as Representative Jerrold Nadler (D-N.Y.) told administration officials during a House Judiciary Committee hearing:

> what we're hearing from this panel, and what we've heard generally about the relevan[ce] standard, is that everything in the world is relevant, and that if . . . we removed that word from the statute . . . the FISA court wouldn't consider that it would affect your ability to collect meta-data in any way whatsoever.

Oversight of the Administration's use of FISA Authorities (comments of Rep. Jerrold Nadler).

Congress charged the FISC with reviewing FBI applications under § 215 to ensure that they comply fully with each of the law's requirements. The FISC's responsibility "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, *supra* § 19:3. Moreover, the FISC cannot delegate this responsibility to intelligence agencies because the FISC's role in granting and overseeing applications is the cornerstone of § 215. As this Court wrote in the case that led to the creation of FISA:

> The Fourth Amendment contemplates a prior judicial judgment, not the risk that executive discretion may be reasonably exercised. This judicial role accords with our basic constitutional doctrine that individual freedoms will best be preserved through a separation of powers

> and division of functions among the different branches and levels of Government.

United States v. United States District Court, 407 U.S. 297, 317 (1972) (citation omitted).

Even before the 2006 amendments added the requirements that an application be "relevant to an authorized investigation," legal experts believed that § 215 authorized data collection and analysis only about specific individuals. In 2003, then-Secretary of Defense Donald Rumsfeld appointed a "blue ribbon" bipartisan independent committee of distinguished attorneys to examine privacy and security issues following the controversy over Total Information Awareness—a prior government program designed to gather comprehensive records of individuals to combat terrorism. *See* Ronald D. Lee & Paul M. Schwartz, *Beyond the "War" on Terrorism: Towards the New Intelligence Network*, 103 MICH. L. REV. 1446, 1467 (2005).

After hearing from 60 witnesses and consulting extensively with legal experts in the DOD, NSA, and other agencies, the Technology and Privacy Advisory Committee ("TAPAC") recommended that Congress should empower the FISC to review applications not only for specific searches, but also for broad data mining programs involving the data of U.S. persons—exactly what the government says it is doing under the Verizon Order. Critically, however, TAPAC concluded that "[l]egislation will be required for the [FISC] to fulfill the role we recommend." TECH. AND PRIVACY ADVISORY COMM., U.S. DEP'T OF DEF., SAFEGUARDING PRIVACY IN THE FIGHT AGAINST

TERRORISM 47 (2004) ("TAPAC Report"). Secretary Rumsfeld accepted TAPAC's recommendation in full, *see* U.S. DEP'T OF DEFENSE, TAPAC RECOMMENDATION WITH IOB RECOMMENDATIONS (Aug. 15, 2006), but Congress never enacted the necessary legal changes.

Indeed, since the TAPAC report was published in 2004, Congress has focused the requirements of § 215 more closely on specific individuals, rather than broad data collection, by requiring that applications for FISA orders include: (1) a statement of facts, establishing "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) . . . ." and (2) compliance with minimization procedures. USA PATRIOT Improvement and Reauthorization Act of 2005 § 106.

The Verizon Order effectively eliminates the relevancy requirement by directing Verizon to disclose all call detail records and telephony metadata, even though the overwhelming majority is, by the government's admission, "never going to be responsive". *NSA Surveillance Leaks: Facts and Fiction* (statement of Robert Litt). Given the scope of records that may be obtained under § 215, the government's rewriting of FISA, which the Verizon Order endorses, grants the government power to gather virtually unlimited data on the daily activities of all U.S. persons. Section 215 cannot be read to authorize such a vast surveillance enterprise.

B. The Verizon Order is Contrary to Executive Order 12333 and the *Attorney General's Guidelines*

In addition to meeting the relevancy requirement, 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).

Executive Order 12333 establishes rules governing U.S. intelligence activities. *See* Exec. Order No. 12333, 46 Fed. Reg. 59941 (Dec. 4, 1981). According to that Executive Order, as amended, "[t]he 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. 12333 § 1.1(b). To fulfill this "solemn obligation," the Executive Order requires intelligence agencies to "use the least intrusive collection techniques feasible within the United States or directed at U.S. persons abroad." § 2.4.

The *Attorney General's Guidelines* reiterate this requirement: "it is axiomatic that the FBI must conduct its investigations and other activities in a lawful and reasonable manner that respects liberty and privacy and avoids unnecessary intrusions into the lives of law-abiding people." ATTORNEY GENERAL'S GUIDELINES at 5. The *Guidelines* expressly state that the "least intrusive method feasible" shall be used in investigations. *Id.* at 12.

Given that the DNI and the DOJ have acknowledged that the NSA never uses the vast majority of call detail records and telephony metadata collected under the Verizon Order, it is unclear how the collection could comply with the "solemn obligation" that the government "use the least intrusive collection techniques feasible," Exec. Order No. 12333 § 1.1(b), 2.4., or how the government's conduct "respects liberty and privacy and avoids unnecessary intrusions into the lives of law-abiding people." ATTORNEY GENERAL'S GUIDELINES at 5.

Quite the contrary, the Verizon Order authorizes collection of call detail records and telephony metadata on law-abiding people for a wholly unnecessary purpose because the government never uses, and knows it will never use, data about the vast majority of Verizon customers and the people who call them.

C. The Investigation is Being Conducted "Solely Upon the Basis of Activities Protected by the First Amendment to the Constitution" in Violation of Section 215

In the case of tangible things sought about a U.S. person, § 215 in two places prohibits conducting an investigation "solely upon the basis of activities protected by the first amendment to the Constitution." 50 U.S.C. §§ 1861(a)(1), (a)(2)(B). The *Attorney General's Guidelines* repeat and expand upon this requirement: "These Guidelines do not authorize investigating or collecting or maintaining information on United States persons solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights

secured by the Constitution or laws of the United States." ATTORNEY GENERAL'S GUIDELINES at 13.

To generate call detail records and telephony metadata covered by the Verizon Order a U.S. person must do only one thing: place or receive a telephone call on a Verizon network. According to this Court, the First Amendment fully protects communication by telephone. *See, e.g.*, *Sable Communications of Calif. v. FCC*, 492 U.S. 115 (1989). The Verizon Order compels disclosure of call detail records and telephony metadata created by U.S. persons doing nothing other than exercising their First Amendment right to express themselves. This protected activity ensnares people under the order. The Verizon Order thus violates the plain language of both § 215 and the *Attorney General's Guidelines.*

The First Amendment concerns are real and substantial. Although not including the content of communications, the call detail records and telephony metadata of millions of U.S. persons disclosed under the Verizon Order can be highly revealing in ways that may be intrinsically harmful or chill the exercise of protected liberties. As twenty-six U.S. Senators wrote to DNI Clapper on June 27, 2013: "These records [collected under the Verizon Order] can reveal personal relationships, family medical issues, political and religious affiliations, and a variety of other private personal information." Letter from Twenty-Six Senators to the Hon. James Clapper, June 27, 2013.

This Court has recognized the danger to expression posed by government surveillance, especially in the national security context: "Though the investigative duty of the executive may be

stronger in such cases, so also is there greater jeopardy to constitutionally protected speech." *United States District Court*, 407 U.S. at 313-14; *see also 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.").

CONCLUSION

For the reasons discussed above, the Verizon Order violates the language and logic of 50 U.S.C. § 1861, and permits the federal government to engage in the unlawful wholesale collection of personal information about U.S. persons.

The government's claims that it is lawful under § 215 for the NSA to determine relevance when it accesses a collected record, rather than having the FISC evaluate relevance when the NSA seeks authorization to collect records, and that hundreds of billions of records are relevant to an investigation simply because they might contain some relevant information, ignore the plain language and purpose of the statute. Nor does the government's approach comply with the "solemn obligation" to "use the least intrusive collection techniques feasible," Exec. Order No. 12333 §§ 1.1(b), 2.4., and "respect[] liberty and privacy and avoid[] unnecessary intrusions into the lives of law-abiding people." ATTORNEY GENERAL'S GUIDELINES at 5.

Finally, the Verizon Order compels the disclosure of call detail records and telephony

metadata that exist only because U.S. persons exercised their First Amendment rights. This violates § 215's prohibition against conducting an investigation "solely upon the basis of activities protected by the first amendment to the Constitution." 50 U.S.C. §§ 1861(a)(1), (a)(2)(B).

The Verizon Order warrants the extraordinary remedy of mandamus because it clearly violates the law and presents a significant risk to the personal privacy of millions of U.S. persons. Such sweeping collection of data about individuals who "have done nothing to warrant government suspicion . . . has the potential to be a 21st-century equivalent of general searches." TAPAC Report at 49. The plain language of § 215 makes clear that Congress denied this virtually unlimited authority to the government, and denied the FISC the power to authorize it.

Respectfully submitted,

FRED H. CATE
Counsel of Record
INDIANA UNIVERSITY
MAURER SCHOOL OF LAW
211 S. Indiana Avenue
Bloomington, IN 47405
(812) 855-1161
fcate@indiana.edu