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* CATO INSTITUTE IN SUPPORT OF PETITIONER

JAMES W. HARPER
Counsel of Record
Cato Institute
1000 Mass. Ave., N.W.
Washington, DC 20001
(202) 842-0200
jharper@cato.org

RANDY BARNETT
Georgetown University
Law Center
600 New Jersey Ave.,
N.W.
Washington, DC 20009
202-662-9936

Counsel for Amicus Curiae

QUESTION PRESENTED

1. Whether the Foreign Intelligence Surveillance Court exceeded its 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.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Constitutional Provisions

Statutes

Other Authorities

INTEREST OF *AMICUS CURIAE*[1]

The Cato Institute was established in 1977 as a nonpartisan public policy research foundation dedicated to advancing the principles of individual liberty, free markets, and limited government. Toward those ends, the Cato Institute publishes books and studies, conducts conferences and forums, and files amicus briefs. This case is of central concern to the Cato Institute because it addresses important statutory and constitutional issues affecting the privacy of law-abiding Americans.

SUMMARY OF ARGUMENT

This case presents the Court with the challenge and opportunity to correct serious statutory and constitutional error that daily deprives millions of law-abiding Americans of their rightful privacy. An order issued under the Foreign Intelligence Surveillance Act requires telecommunications company Verizon on an "ongoing, daily basis" to give the National Security Agency information on all telephone calls in its systems, both within the U.S. and between the U.S. and other countries.

This order is contrary to the statute under which it was issued and unconstitutional under the Fourth

---

[1] Pursuant to this Court's Rule 37.3(a), letters of consent from all parties, having been given timely notice to the filing of this brief, have been submitted to the Clerk. Pursuant to this Court's Rule 37.6, *amicus* states that this brief was not authored in whole or in part by counsel for any party, and that no person or entity other than *amicus* or its counsel made a monetary contribution intended to fund the preparation or submission of this brief.

Amendment. And this order was issued without according due process to the parties affected.

Two terms ago, this Court in *Jones v. United States* speculated about the potential of recent growth in the use of information technology to undercut traditional constitutional protections of privacy. Sooner than expected, this potential has become all too real. By granting the petition in this case, this Court can confront and correct the immediate statutory and constitutional issues. And it is now time for the Court to reassess *Smith v. Maryland* and the "third-party doctrine," which have precipitated a juridical privacy crisis.

ARGUMENT

I. THE VERIZON ORDER IS INCONSISTENT WITH THE PLAIN MEANING OF THE STATUTE AND CONGRESSIONAL INTENT IN PASSING IT

The USA-PATRIOT Act does not permit the government's order requiring Verizon to disgorge data about every American's telephone calls every day (hereinafter, the "Verizon order"). Its precise language, Congress's intent in enacting it, and the structure of the law all cut against the order. Yet the Electronic Privacy Information Center (hereinafter, "EPIC") has no recourse besides this Court.

A. The plain meaning of the statute requires an investigation to preexist any § 215 order, with relevance judged according to the contours of that investigation

Section 215 of the USA-PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272, amended the Foreign Intelligence Surveillance Act ("FISA") to require FISA judges to issue orders (hereinafter "§ 215 orders") requiring the production of tangible things upon satisfactory application by the Federal Bureau of Investigation. The language of the statute, codified at 50 U.S.C. § 1861, requires there to be an investigation in existence at the time such a judge issues a § 215 order. Because the Verizon order does not pertain to an existing investigation, it is not authorized by the statute.

Section (b) of 50 U.S.C. § 1861 specifies that an application for a § 215 order 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). In two ways, this language requires an investigation to pre-exist any such application.

First, the required statement of facts must show that the things sought "*are* relevant" to an investigation. "Are" is the present participle (plural) of the verb "to be." It requires a showing at the time of application that the things sought are relevant to an investigation.

This presumes and requires the existence of an investigation at the time of application. "Investigation" is the process of inquiring into or tracking down through inquiry. Black's Law Dictionary 825 (6th ed. 1990). "Relevancy" is "that which conduces to the

proof of a pertinent hypothesis." Black's Law Dictionary 1290 (6th ed. 1990). There can be no pertinence without a hypothesis.

Given the impossibility of showing relevance to an investigation that does not yet exist, it is impossible for a FISA judge to have found that the Verizon application met the requirements of the law. It cannot seriously be contended that all telephone records produced by a major U.S. telecommunications provider are for the kind of directed, pre-existing inquiry denoted by the terms Congress used.

Congress could have permitted the FBI to apply for § 215 orders relating to anticipated investigations by using the future tense or any number of auxiliary verbs, such as "can"; "could"; "will"; or "might." But it chose not to do so. Instead, Congress required relevance to an investigation existing at the time of the application.

Second, the statement of facts required by 50 U.S.C. § 1861(b)(2)(A) must show that the application is relevant to an "authorized" investigation. "Authorized," the past participle of "to authorize," is an adjective modifying the word "investigation." It requires something to have happened to the investigation—its authorization—before it can be the basis of a satisfactory application.

As with relevance, it is impossible to determine that an investigation is or has been "authorized" if the investigation has not come into existence. Therefore, it is impossible for a FISA judge to have properly concluded that an application for a *future* investigation met the standards of the statute.

Because the Verizon order does not pertain to an existing investigation, it violates the plain language of the statute.

B. Congress intended § 215 orders to pertain to existing investigations

In passing § 215, Congress did not intend to create authority for collection of information beyond that which is relevant to an existing investigation. Although the final version of the USA-PATRIOT Act did not include report language stating its intent, report language accompanied a precursor of § 215, and it clarifies Congress's purposes.

Section 156 of H.R. 2975 was entitled "Business Records," and provided for applications to FISA judges similar to what Congress incorporated into the final version of the USA-PATRIOT Act. The report for that bill discussed its business records provision as follows:

> The Administration had sought administrative subpoena authority without having to go to court. Instead, section 156 amends title 50 U.S.C. § 1861 by providing for an application to the FISA court for an order directing the production of tangible items such as books, records, papers, documents and other items upon certification to the court that the records sought are *relevant to an ongoing foreign intelligence investigation*. H.R. Rep. No. 107-236, 107th Cong., 1st Sess., pt. 1, at 61 (2001) (emphasis in original).

This reaffirms that the grammatical reading of the final text is correct: By its choice of language, Congress did not intend to allow applications with potential relevance to foreign intelligence generally; in-

stead it intended to restrict them to pre-existing, "ongoing" investigations.

After the Verizon order was revealed, Rep. F. James Sensenbrenner, chairman of the House Judiciary Committee when the USA-PATRIOT Act passed, confirmed the purposes embodied in the text of § 215. "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? This is well beyond what the Patriot Act allows." Rep. Jim Sensenbrenner, *This Abuse of the Patriot Act Must End*, The Guardian (U.K), June 9, 2013.

From the time of the USA-PATRIOT Act's passage to the present day, the intent of Congress and its members, as reflected in the law's text, was to authorize applications that were relevant to existing, discreet investigations, not applications for general surveillance with potential relevance to possible future investigations.

C. The statute explicitly bars narrower uses of information than the Verizon order permits, suggesting that the drafters of the statute did not anticipate orders like the Verizon order

Other evidence of meaning in § 215 suggests that Congress did not intend to permit orders with the broad sweep of the Verizon order.

Congress excluded threat assessments from the ambit of § 215 orders. 50 U.S.C. § 1861(b)(2)(A) (application must show that "things sought are relevant to an authorized investigation (other than a threat

assessment)"). Threat assessments range from background check systems, *e.g.*, 6 U.S.C. § 924, to general studies that analyze trends, patterns, probabilities, and responses to terrorism and crime, *e.g.*, 42 U.S.C. § 3714a. Although relevant to what could be considered "investigations" in a broad sense, Congress nevertheless denied permission to obtain § 215 orders for such uses. This denial is inconsistent with the claim that an even broader, undifferentiated collection of data is within the scope of § 215. How can the statute require FISA judges to approve the collection of data about the phone calling of innocent American retirees in support of possible future investigations, while it bars them from approving § 215 applications that will gather data for specific background checks on people holding sensitive positions in the government or private sector?

D. The unlimited § 215 order effectuates a data retention policy that Congress has declined to establish, and it skirts congressional policy around pen registers

This Court should refuse FISA judges the authority to transmogrify § 215 into a data retention program that Congress has debated and refused to approve or into a pen register policy different from the one Congress has established in law.

Since at least 2006, administration officials representing both recent presidents have sought legislation requiring telecommunications providers and Internet service providers to retain data about their customers' activities so the government can acquire such data if those customers later come under suspicion of wrongdoing. *See* Ryan Paul, *Attorney General Gonzales Talks Up Data Retention*, Ars Technica,

Sept. 20, 2006, http://tinyurl.com/CatoNSA1; Declan McCullagh, *FBI, Politicos Renew Push for ISP Data Retention Laws*, C|Net News, Apr. 23, 2008, http://tinyurl.com/CatoNSA2; Declan McCullagh, *DOJ Wants Mandatory Data Retention*, CBSNews.com, Jan. 25, 2011, http://tinyurl.com/CatoNSA3.

Members of Congress have introduced bills to institute mandatory data retention policies, nominally for the purpose of controlling child exploitation. *See*, *e.g.*, H.R. 837, 110th Cong., 1st Sess. § 6 (2007); H.R. 1076, 111th Cong., 1st Sess. § 5 (2009); S. 436, 111th Cong., 1st Sess. § 5 (2009); H.R. 1981, 112th Cong., 1st Sess. § 4 (2011). But in 2012 Congress enacted child protection legislation similar to these proposals but *without* a data retention mandate. Child Protection Act of 2012, Pub L. No. 112-206, 126 Stat. 1490.

Congress has declined to institute mandatory data retention laws because the costs, risks, and privacy consequences for innocent citizens outweigh their law enforcement and security benefits. The Verizon order reverses this Congressional policy by requiring a telecommunications provider to turn all data over to the government for retention by the National Security Agency.

The Verizon order also facilitates a pen register policy different from the one Congress has established in law. The combination of prospective collection with the "automated query process" described in the "primary order" effectively creates a pen register. (To mount a political defense of the Verizon order, the government on July 31, 2013, declassified the "Primary Order" that preceded the Verizon order. *See In re: Application of the Federal Bureau of Investigation*

for an Order Requiring the Production of Tangible Things from [redacted] (FISC) (Docket No. BR), (Apr. 25, 2013).) This circumvents the separate authority at 50 U.S.C. § 1842 that Congress intended to be used for monitoring of this kind.

As described in the primary order, the typical use of this database involves a list of flagged query terms—primarily, though not exclusively, phone numbers—which are run against the updated database each day, with the results fed into a "corporate store" for future analysis. That is the definition of a pen register: a "device or process" used to prospectively and continuously obtain routing or signaling information. *See* 18 U.S.C. § 3127(3).

Under the primary order, a particular search term (phone number) may be automatically queried upon a finding of reasonable suspicion for up to 180 days—double the maximum length of time Congress allows for pen registers, 50 U.S.C. § 1842(e). (Congress allows a longer duration only when the information sought is "foreign intelligence information not concerning a United States person," 50 U.S.C. § 1842(e)(2), a condition unlikely to be met by queries of a database containing domestic call records.) Section 1842 clearly stipulates that pen register orders must identify the particular facilities (phone lines or accounts) to which they apply, 50 U.S.C. § 1842(d)(2), a limitation the primary order and the Verizon order ignore.

The government cannot simply choose to bypass the specific process Congress established for monitoring via pen register by splitting the process into two steps (step one: daily bulk collection of all telephone calling data; step two: copying of the flagged devices

into the working database or "corporate store"). The government has effectively used § 215 to create a back door pen register because it found the constraints Congress imposed on statutory pen register authority in 50 U.S.C. § 1842 inconvenient.

Given clear statutory language, congressional intent, the structure of the statute, congressional aversion to data collection and retention, and pen registers law which the Verizon order evades, this Court must find that the Verizon order is not authorized by § 215.

II. THE VERIZON ORDER IS UNCONSTITUTIONAL

Should the Court find that the Verizon order is authorized by the statute, it must decide whether the order complies with the Fourth Amendment. Because the blanket seizure of privately maintained data was upheld in a secret proceeding conducted by the FISA panel, we are compelled to speculate about the legal theory under which it was upheld. The order is unconstitutional under any theory.

If the Verizon order is a warrant, it is a general warrant, which is flatly banned by the Fourth Amendment. If the order is a subpoena or any other form of mandate, it is unreasonable and thus unconstitutional on that basis.

A. The Verizon order is a general warrant, which is flatly banned by the Fourth Amendment to the U.S. Constitution

The Fourth Amendment has two parts: First, "The right of the people to be secure in their persons,

houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV. And second, "no warrants shall issue, but upon probable cause, supported by oath or affirmation, and *particularly describing the place to be searched, and the persons or things to be seized*." *Id*. (emphasis added). Whether the latter sentence is an example of unreasonableness or a freestanding ban, general or nonspecific warrants are what the Fourth Amendment was adopted to prevent.

The Fourth Amendment requires the things to be searched or seized under a warrant to be described "particularly." A thing is "particular" if it relates "to a part or portion of anything," if it is "individual; specific; local; comprising a part only; partial in extent; [and] not universal." Black's Law Dictionary 1119 (6th ed. 1990). The Verizon order requires Verizon to produce "on an ongoing daily basis … all call detail records." That is not "particular."

The Verizon order is the modern incarnation of the "general warrants" issued by the Crown to authorize searches of American colonists. The Founders' condemnation of general warrants applies very well to the Verizon order and any other "programmatic" collection authorities the government may claim.

In one of the three seminal cases historians regard as the inspiration for the Fourth Amendment, *Entick v. Carrington*, 19 Howell's State Trials 1029 (1765), Lord Camden explained why general warrants are abhorrent in terms that could be used to characterize the Verizon order:

> [The general warrant] is executed by messengers with or without a constable (for it can never be pretended, that such is necessary in point of law)

> in the presence or the absence of the party, as the messenger shall think fit, and without a witness to testify what passes at the time of the transaction; so that when the papers are gone, as the only witnesses are the trespassers, the party injured is left without proof.
>
> If this injury falls upon an innocent person, he is as destitute of remedy as the guilty: and the whole transaction is so guarded against discovery, that if the officer should be disposed to carry off a bank bill he may do it with impunity, since there is no man capable of proving either the taker or the thing taken. 19 Howell's State Trials at 1064-66.

With general warrants many innocent people might be subject to the exposure or seizure of their private papers, without their knowledge and with no realistic prospect of a remedy. This is precisely the risk created by the Verizon order.

Post-seizure "protections" regulating the searches of *already seized* papers, *see In re: Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from* [redacted] (FISC) (Docket No. BR)(Apr. 25, 2013), are no constitutional substitute for either non-seizure or particularized seizures. The blanket and ongoing seizure and retention of data about Americans' phone calls—reflecting their relationships, business contacts, access to legal counsel, and more—are susceptible to future abuses as well as the inevitable failures to abide by existing rules. Such failures have already occurred. Undated letter from Director of National Intelligence James Clapper to Senator Ron Wyden (D-OR), http://tinyurl.com/CatoNSA4 ("…there have been a number of compliance prob-

lems…"). Press reports indicate there may be more. Brian Fung, *The NSA is giving your phone records to the DEA. And the DEA is covering it up*. Washington Post, Aug. 5, 2013, http://tinyurl.com/CatoNSA5. Only the particularized warrant requirements expressed in the Fourth Amendment itself can effectively prevent these abuses from occurring.

As with the First Amendment's protection of "the press," the fact that "papers" are now in digital rather than analog form in no way affects the application of the Fourth Amendment to today's technology. On the contrary, the increased power of government agents to collect, store, survey, and analyze great masses of data with powerful algorithms run on supercomputers only exacerbates the dangers contemplated by James Madison and the first Congress, who proposed the Fourth Amendment, and the states that promptly ratified it.

B. If not a general warrant, the Verizon order is nevertheless unconstitutional because it is "unreasonable"

Any claim that the Verizon order is the equivalent of a judge-signed subpoena, as distinct from a warrant, is contrary to legislative history showing that Congress denied the executive subpoena authority. H.R. Rep. No. 107-236, 107th Cong., 1st Sess., pt. 1, at 61 (2001) (discussing predecessor language to § 215 as denying subpoena authority). And if it is such a thing, this would constitute a type of subpoena previously unknown to the criminal or civil law. Merely substituting the word "subpoena" for "warrant" cannot evade the Constitution's proscription against unreasonable seizures. And a blanket subpoena, like a general warrant, is the sine qua non of "unreason-

able." *See generally* Christopher Slobogin, *Subpoenas and Privacy*, 54 DePaul L. Rev. 805 (2005).

Whether the Verizon order is a warrant or a "subpoena," allowing blanket seizures of data would constitute an unprecedented legal and constitutional seachange that, if undertaken at all, should be undertaken only after robust public debate and a constitutional amendment that is itself worded specifically enough to govern the executive branch in the future. It is not a policy that should emerge from an advisory panel of judges, issuing a secret interpretation of § 215 to which EPIC in particular, and the People in general, are not privy.

III. UNDER *JONES*, EPIC HAS A LEGAL AND CONSTITUTIONAL INTEREST IN DATA ABOUT ITS TELEPHONE CALLS

As *Jones v. United States* reiterated, property is a touchstone of Fourth Amendment protection. 132 S. Ct. 945 (2012). Petitioner EPIC has a legal and constitutional interest in data about its telephone calls resting on both statutory and contract rights. The Verizon order interferes with these rights.

Smith v. Maryland is easily distinguished from the present case, and it was wrongly decided. 442 U.S. 735 (1979). Especially if it controls, this Court should grant the writ in order to reverse *Smith* and revise or repudiate the third-party doctrine, of which *Smith* is a part.

A. *Jones* reiterates that property is a touchstone of Fourth Amendment protection

For good reason, the Fourth Amendment uses a possessive pronoun—"their"—to describe the "persons, houses, papers, and effects" it protects. U.S. Const. amend. IV. People's ownership of themselves and their things is an essential counterweight to state power. The Fourth Amendment has long and appropriately been administered with reference to property.

To some, *Katz v. United States*, 389 U.S. 347 (1967), seemed to replace this Court's previous use of property rights to identify the existence of a search or seizure, substituting instead a person's "reasonable expectation of privacy." But the majority in *Jones* showed that the *Katz* formulation adds additional protection *beyond* the foundation of the Fourth Amendment: protection of one's property. "[T]he Katz reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test." *Jones*, at 952. *See also id.* at 954-55, (Sotomayor, J. concurring) ("Of course, the Fourth Amendment is not concerned only with trespassory intrusions on property. Rather, even in the absence of a trespass, a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." (quotations and citations omitted)).

B. The Verizon order interferes with EPIC's proprietary right, recognized by statute, to control others' access to information about its calls

EPIC has a property interest in the data recording its telephone calling. The Verizon order interferes

with this interest. This Court should grant the writ so that EPIC can have a remedy, none being offered by the FISA panel's appeals process, such as it is.

Property is an age-old common law concept, and Congress did not invent the idea that data can be held as property. But in section 702 of the Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56, Congress added a new section 222 to the Communications Act, 47 U.S.C. § 222, that illustrates the common treatment of communications data as property. It says: "Every telecommunications carrier has a duty to protect the confidentiality of *proprietary information* of, and relating to, other telecommunication carriers, equipment manufacturers, and customers…." 47 U.S.C. § 222(a) (emphasis added).

The statute defines "Customer Proprietary Network Information" ("CPNI"), as "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 … information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer…." 47 U.S.C. § 222(h)(1).

Congress used the word "proprietary" to refer to this information. It clearly conceived of the collections of information that telephone companies amass as items of property.

Doing so does not exclude the same information being property of the customer, in the same form or another. Indeed, the statute allocates some narrow statutory property rights in CPNI to customers of tel-

ecommunications firms. For example, consumers can require telecommunications providers to disclose copies of their CPNI. 47 U.S.C. § 222(c)(2). The information is "theirs" if they want it. The privacy requirements of the statute can be avoided "with the approval of the customer," 47 U.S.C. § 222(c)(1), meaning that the information controls in the statute are alienable, as property rights are.

Where the statute provides that its protections can be overcome "as required by law," 47 U.S.C. § 222(c)(1), this gives EPIC a statutory right against the government seizing information if that seizure is not "required by law." EPIC alleges correctly that the Verizon order violates the law.

A second fount of legal protection for EPIC's communications information is private law. Verizon's privacy policy, Verizon, *Full Privacy Policy* Web page, Mar. 2013, http://tinyurl.com/CatoNSA6, current at the time of disputed data collection under the Verizon order, is a 5,000-word tome, describing in detail the company's policies with regard to data collection, use, sharing, safety, and security. Among many other things, it provides: "We may disclose information that individually identifies our customers or identifies customer devices in certain circumstances, such as: to comply with valid legal process including subpoenas, court orders or search warrants, and as otherwise authorized by law…." *Id.*

Through painstaking common law development, our society is determining the role of online statements, "clickwrap" licenses, and such in creating legally binding obligations. *See* Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's*

Action Against Sears, 8 Nw. J. Tech. & Intell. Prop.1 (2009). The better view is that privacy policies and published Terms of Use statements are either explicit contract terms or attempts by the supplying party to establish, augment, or alter implied contract rights.

The Verizon privacy policy promises EPIC to disclose data only based on valid legal process. EPIC has a legal interest in preventing disclosures based on invalid legal process, and this Court should allow it to contest the statutory and constitutional validity of the Verizon order.

C. This case is distinguishable from *Smith v. Maryland*

The argument that EPIC does not have an interest in its data is based on the "third-party doctrine" as applied in *Smith v. Maryland*, 442 U.S. 735 (1979). In *Smith*, the Court held that using a pen register or trap-and-trace device (which records the numbers dialed from, and dialing to, a particular phone) was not a Fourth Amendment "search." However, the facts and circumstances in *Smith* differ markedly from this case.

In *Smith,* police had information strongly indicating that a man who had burglarized a home was calling its occupant and harassing her. At their request, the telephone company installed a pen register to record the numbers dialed from his telephone. 442 U.S. 735, at 737. The Court found that no warrant was required. 442 U.S. at 746.

This case, by contrast, involves mass surveillance, the gathering of data on everyone including members of this Court, and in digital form, which is highly susceptible to advanced processing, such as network

analysis and predictive data mining. This can reveal troves of information about vast numbers of non-suspects: relationships, actions, habits, medical/psychological treatments, legal counsel, business decisions, political negotiations, and more.

Sporadic use of pen registers and trap-and-trace devices does not permit the inferences that large datasets do. Even if it was "reasonable" to install a pen register on one person's land-line phone in 1979, that does not make it reasonable to collect and store data about all Americans' phone calls, making such data available to the government for algorithmic analysis, today. *Smith* is too unlike this case to provide a binding precedent.

D. *Smith v. Maryland* was wrongly decided, and the "third-party doctrine" is an anachronism

Assuming it finds *Smith* controlling, *Smith* should be reversed. This Court should reconsider the third-party doctrine and either adapt it to modern circumstances, as Justice Sotomayor has suggested, or reject it altogether.

Smith v. Maryland was a classic "reasonable expectation of privacy" case, and a paragon of its maladministration. *Smith* purported to follow the reasoning of Justice Harlan's solo-concurrence in *Katz*:

> My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable. *Katz*, 389 at 361.

In his opinion in *Smith*, however, Justice Blackmun inaccurately applied this doctrine. The question whether a person has an actual (subjective) expectation of privacy is a question of fact, but the Court treated it as an objective question, denying the possibility of such an expectation. *Smith*, 442 at 743 ("[I]t is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret."). Having misapplied the subjective part of the *Katz* test, the Court appears also to have botched the objective part. Justice Blackmun marshaled arguments for the position that an expectation of privacy is unreasonable, but made no comparing or contrasting mention of counterarguments. *Smith*, 442 U.S. at 744-45. Most likely, he treated the objective part of the *Katz* test subjectively, universalizing his own opinion as though it were the one true opinion on privacy around telephone dialing information.

Having misapplied the *Katz* test, the Court arrived at the wrong result. Phone calling information is available to the phone company and a contained universe of service providers. At the same time, however, common experience shows that phone companies keep it private from everyone else: friends, neighbors, teachers, co-workers, passers-by, postal workers, plumbers, and painters. Similarly, the public reasonably assumes these records are kept from government agencies absent a warrant.

Smith v. Maryland should be reversed because it was badly reasoned. And the third-party doctrine, of which *Smith* is an exemplar, should be repudiated as an unrealistic misapplication of the "reasonable ex-

pectation of privacy" rationale of *Katz*. As Justice Sotomayor noted in *Jones*:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.... I would not assume that all information voluntarily disclosed to some member of the public *for a limited purpose* is, for that reason alone, disentitled to Fourth Amendment protection. *Jones*, at 957 (Sotomayor, J., concurring) (emphasis added; citation omitted).

The fixing of a GPS tracker to a single person's automobile in *Jones* did not squarely present the issues that gave rise to Justice Sotomayor's concerns. The blanket seizure, long-term storage, and exposure to algorithmic analysis of EPIC's communications data unquestionably do.

Yesterday's tomorrow has already arrived. *Smith v. Maryland* and the third-party doctrine are inapt for these times. This Court should not allow the third-party doctrine to permit blanket seizures of data that has been disclosed to a third party under contractual and regulatory restrictions.

E. This Court should use a judicially-administrable property- and contract-based approach to the Fourth Amendment's protection of private communications

Rather than airy judicial speculations about "reasonable expectations" of the sort entertained by Justice Blackman, this Court should return to the traditional—and more readily administrable—property and contract rights focus of Fourth Amendment. In *Jones*, this Court took an important step in this direction. It should now recognize the privacy of communications data that has *in fact*, in the words of the Fourth Amendment, been "secure[d]" by sufficient physical and legal protections.

Having employed written communications, both public and private, to revolutionize political life on the American continent, protecting private information from the prying eyes of government was a priority for the Founders. Anuj C. Desai, *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, 60 Stan. L. Rev. 553, 564 (2007). Congress's first comprehensive postal statute wrote the confidentiality of sealed correspondence into law with heavy fines for opening or delaying mail. *Id.* at 566-67; Act of Feb. 20, 1792, § 16, 1 Stat. 232, 236. This Court validated Fourth Amendment protection for mail in *Ex Parte Jackson,* 96 U.S. 727 (1877), though possession of the information therein was given to the government itself, secured only by a seal on a paper envelope.

The very year this Court decided *Ex Parte Jackson*, both Western Union and the Bell Company began establishing voice telephone services. Gerald W.

Brock, The Second Information Revolution 28 (Harvard University Press, 2003). Now, instead of written messages in the post, representations of the human voice itself began moving across distance, at light speed, in a way few people understood. This is the technology this Court confronted in *Olmstead v. United States*, 277 U.S. 438 (1928).

The Court handled this technological development poorly. Chief Justice William Taft fixed woodenly on the material things listed in the Fourth Amendment's search and seizure clause. Because wiretapping had not affected any of the defendants' tangible possessions, he found it did not affect their Fourth Amendment rights. *Olmstead,* 277 U.S. at 464. In dissent, however, Justice Butler noted how "contracts between telephone companies and users contemplate the private use" of telephone facilities. *Olmstead*, 277 U.S. at 487 (Butler, J., dissenting). Like private letters entrusted to the Post Office, the "communications belong to the parties between whom they pass," he said. *Id. Cf. Ex Parte Jackson*, 96 U.S. 727 (1877)("Letters and sealed packages … are as fully guarded from examination and inspection … as if they were retained by the parties forwarding them in their own domiciles.").

Nearly forty years later in *Katz*, the Court found Fourth Amendment protection for a conversation that would have at an earlier time been held in the home, office, or other secluded environment. *Katz*, 389 U.S. at 352. To replicate that seclusion, Charles Katz had shielded the sound of his voice from others in a phone booth, even though in a public place. *Id*. By taking these steps to shield his voice from others, Katz created the "reasonable expectation of privacy" to which

Justice Harlan's solo concurrence refers. So too does sealing a letter before handing it to the postman, putting one's email behind a password, or using a communications company with a privacy policy.

This Court should refine its doctrine to replace judicial speculations with affirmation that the physical and legal barriers people place around their information define both their actual and "reasonable" expectations of privacy. To overcome these barriers, the Constitution requires the government must obtain a warrant defined by the Fourth Amendment.

IV. EPIC AND VERIZON ARE BEING DEPRIVED OF PROPERTY WITHOUT DUE PROCESS OF LAW

Upon accepting EPIC's petition, this Court may also consider whether the procedures established by the Foreign Intelligence Surveillance Act provide communications companies and their customers the "due process of law" required by the Fifth Amendment.

Although judges historically have approved individual search warrants, later subject to review in a contested proceeding, here the constitutionality of a massive program of data seizure is being adjudicated in secret. Neither EPIC nor any other Verizon customer has the right to intervene and contest the case, much less read the decision purporting to uphold the constitutionality of the seizure of its data.

In the seminal case on the role of federal courts, this Court ruled: "A case or controversy, in order that the judicial power of the United States may be exercised thereon, implies the existence of present or pos-

sible adverse parties whose contentions are submitted to the court for adjudication. *Chisholm v. Georgia*, 2 Dall. 431." *Muskrat v. United States*, 219 U.S. 346 (1911). The Foreign Intelligence Surveillance Court is unlike any other Article III court and is more accurately conceived of as an advisory body. Both Verizon and EPIC are being deprived of their property in secret proceedings, with orders justified by secret opinions. This is the antithesis of the Due Process of Law that is guaranteed by the Fifth Amendment.

CONCLUSION

In a republican form of government based on popular sovereignty, the people are the principals or masters and those in government are their agents or servants. For the people to control their servants, they must know what their servants are doing. The secrecy of these programs and the proceedings by which their constitutionality is assessed make it impossible to hold elected officials and appointed bureaucrats accountable.

Relying solely on internal governmental checks violates the fundamental constitutional principle that the sovereign people must be the ultimate judge of their servants' conduct in office. Such judgment and control is impossible without the information that secret programs conceal. Had it not been for recent leaks, subsequently confirmed by the government, the American public would have no idea of the existence of these programs, and we still cannot be certain of their scope.

What we know of them reveals that they are contrary to statute, and unconstitutional under any the-

ory. Yet, every day, the ongoing Verizon order deprives millions of Americans of privacy.

Only a writ of mandamus can provide the American people in general, and EPIC and Verizon in particular, with relief from this unprecedented surveillance of them by their servants.

Respectfully submitted,

JAMES W. HARPER
Counsel of Record
Cato Institute
1000 Mass. Ave., N.W.
Washington, DC 20001
(202) 842-0200
jharper@cato.org

RANDY BARNETT
Georgetown University
Law Center
600 New Jersey Ave.,
N.W.
Washington, DC 20009
202-662-9936

Counsel for Amicus Curiae

AUGUST 12, 2013