No. 12-3052; Consolidated with Nos. 12-3053, 12-3054

IN THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v.

KENNETH BENBOW; MARK PRAY; ALONZO MARLOW,
Defendants-Appellants.

On Appeal from the United States
District Court for the District of Columbia

BRIEF OF THE CATO INSTITUE AS *AMICUS CURIAE* IN SUPPORT OF APPELLANTS

Ilya Shapiro
Counsel of record
Jim Harper*
Randal J. Meyer*
CATO INSTITUTE
1000 Mass. Ave., N.W.
Washington, D.C. 20001
(202) 842-0200
ishapiro@cato.org
jharper@cato.org
rmeyer@cato.org
*Admission pending

August 26, 2016

COMBINED CERTIFICATES

Certificate as to Parties, Rulings, and Related Cases

Per Circuit Rule 28(a)(1), counsel for *amicus* Cato Institute ("Cato") certify as follows: All parties, intervenors, and *amici* that have appeared in this Court are listed in the Appellant's Brief; Cato will be listed in the finalized Appellant's Brief. The rulings at issue and related cases also appear in the Appellant's Brief.

Certificate of Counsel under Circuit Rules 29(c)(4) and 29(c)(5)

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, Cato publishes books and studies, conducts conferences, and issues the annual *Cato Supreme Court Review*. Cato files this brief to address the implications of radically expanding the third-party doctrine to undermine privacy interests protected by property rights under *Katz* and *Riley*—issues that no other *amicus* brief covers.

Corporate Disclosure Statement

Pursuant to FRAP 26.1, the Cato Institute certifies that it has no parent corporation, and no publicly held company has 10% or greater ownership in it. All parties to the named and consolidated cases have consented to this filing.

/s/ Ilya Shapiro
Ilya Shapiro
Counsel for *Amicus Curiae*

TABLE OF CONTENTS

TABLE OF AUTHORITIES

* Authorities upon which we chiefly rely are marked with an asterisk.

Cases

Constitutional Provisions

Statutes

Other Authorities

Regulations

GLOSSARY

SCA – Stored Communications Act

CSLI – Cell Site Location Information

INTRODUCTION AND INTEREST OF *AMICUS CURIAE*[1]

The Cato Institute is a nonpartisan public-policy foundation dedicated to individual liberty and free markets. Cato's Center for Constitutional Studies promotes the limited, constitutional government that is the foundation of liberty. This case concerns Cato because it implicates core Fourth Amendment interests.

The Fourth Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and 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." U.S. Const. amend. IV.

Here, the government seized the CSLI data, which was unavailable to it other than by invoking legal processes that threatened punishment for non-compliance. *See generally Microsoft v. United States*, No. 14-2985, 2016 U.S. App. LEXIS 12926 (2d Cir. July 14, 2016) (civil contempt action for failure to comply with §2703 warrant). Through this seizure, the government gained access to a constitutionally protected paper or effect without meeting the warrant standard. The third-party doctrine provides no exception to that requirement here.

---

[1] No one other than the *amicus* and its counsel wrote this brief in whole or in part. The cost of its preparation was paid solely by *amicus*.

SUMMARY OF ARGUMENT

The lower court erred in finding that the court-ordered seizure of Alonzo Marlow's cell site location information (CSLI) under the Stored Communications Act (SCA), 18 U.S.C. § 2703(d), did not violate the Fourth Amendment.

For constitutional purposes, CSLI is a kind of "paper" or "effect," in which Marlow had a contract-based property right, specifically the right to exclude others. Congressional and agency treatment of data and privacy policies accord with treatment of CSLI as property subject to contractual commitments—as do Supreme Court precedents like *United States v. Jones*, 132 S.Ct. 945, 957 (2012), and *Katz v. United States*, 389 U.S. 347 (1967). Seizing the CSLI based on a lower evidentiary showing than would be required for a warrant was thus unreasonable.

Nor does the third-party doctrine allow warrantless seizure of CSLI. That doctrine, a corollary of the "reasonable expectation of privacy" test, has been the subject of sound judicial criticism, and the Supreme Court has eschewed it of late. Notably, the Court did not apply it—or the third-party doctrine—in its most relevant recent cases, *Jones* and *Riley v. California*, 134 S.Ct. 2473 (2014).

Accordingly, this Court should reverse the lower court and hold that CSLI created by individuals in concert with a communications provider—and under contract terms that maintain the individual's property interest in that data—enjoy Fourth Amendment protection, particularly the warrant requirement.

ARGUMENT

I. THE GOVERNMENT SEIZED MARLOW'S CSLI, WHICH IS A PAPER OR EFFECT FOR FOURTH AMENDMENT PURPOSES

When the government has effected a seizure or search, the first question to ask under Fourth Amendment analysis is whether the object of the seizure or search was a constitutionally protected item—a person, house, paper, or effect. Here, the question has two parts: (1) Whether the CSLI was a paper or effect, and (2) whether it belonged to Marlow. The answer to both parts is affirmative.

A. Data Such as CSLI Is a "Paper" or "Effect" for Fourth Amendment Purposes

CSLI is best treated as a constitutionally protected "paper" or "effect." This is a more difficult conclusion to reach than it should be because, even in easy cases, the Supreme Court often leaves to inference that something falls within one of the categories of items the Fourth Amendment covers. The Court has rarely made explicit what the boundaries of the "papers" and "effects" categories are, but its recent *Riley* decision offers helpful direction about how digital files fit into this constitutional categorization.

Riley dealt with the search of a cell phone, bluntly stating that searching a phone requires government agents to "get a warrant." *Riley*, 134 S.Ct. at 2495. By necessary inference, phones themselves are effects. Dictum in *Riley* suggests strongly that digital files are also effects: The *Riley* Court declined to adopt a middle-ground standard urged by the government allowing cell-phone searches if it

is reasonable to believe that a phone contains evidence of the crime of arrest. *Id*. at 2492. The reason was that doing so would "in effect give police officers unbridled discretion to rummage at will among a person's *private effects*." *Id*. (quotation and citation omitted) (emphasis added). The Court treated not just phones, but the digital documents and materials they hold, as effects.

At least one circuit court has found constitutional protection for email, which also must rest on the premise that digital data in the form of an email file is a paper or effect for Fourth Amendment purposes. In *United States v. Warshak*, the Sixth Circuit wrote: "Given the fundamental similarities between email and traditional forms of communications, it would defy common sense to afford emails lesser Fourth Amendment protection. Email is the technological scion of tangible mail." 631 F.3d 266, 285-6 (6th Cir. 2010).

The parallel between emails and tangible mail is the beginning but not the end of the relationship between digital files and the papers/effects categories. Email is but one of many protocols that replicate and expand on people's ability to collect, store, and transmit personal information as they did in the Founding era. There are many protocols that convert text, sounds, images, video, and associated data into digital files and permit their transport via modern equivalents of postal mail. This Court would best treat digital files as papers or effects, regardless of its determinations about the reasonableness of seizing and searching particular files.

The Supreme Court has protected data in a variety of formats under the Fourth Amendment, either directly or because it is appurtenant to protected things. In *Katz v. United States*, 389 U.S. 347 (1967), the Court treated the sound of Katz's voice, suitably shrouded, as a constitutionally protected item. Sound waves are a natural information conveyance equivalent to made items like paper. The best understanding of *Katz* consistent with the text of the Fourth Amendment is that a whisper or shrouded oral communication is an "effect." *Kyllo v. United States* similarly gave protection to information in the form of analog infrared waves because of its appurtenance to a house. 533 U.S. 27, 40 (2001).

One scholar has found that each of the items singled out for protection in the Fourth Amendment has been given "a more expansive reading than the pre-technological and pre-industrial world of the Founders." Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 Cal. L. Rev. 101, 150 (2016). The concept of "papers and effects" must be interpreted in light of changed technologies. It was not papers as a form-factor for cellulose that the Framers sought to protect, of course, but as a commonly used medium for storage and communication of information. *See United States v. Seljan*, 547 F.3d 993, 1014-17 (9th Cir. 2008) (Kozinski, J., dissenting) ("What makes papers special—and the reason why they are listed alongside houses, persons and effects—is the ideas they embody, ideas that can only be seized by reading the

words on the page."), *cert. denied*, 129 S.Ct. 1368 (2009). Digital documents and files are papers. As someone's property, they are effects.

The federal judiciary has recognized, as it must, that digital representations of information are equivalent to paper documents for purposes of both filing and discovery. *See* Committee on Rules of Practice and Procedure of the Judicial Conference of the United States, Report of the Civil Rules Advisory Committee 2, 18-22 (2005), available at http://www.uscourts.gov/file/14746/download. The subject matter commonly held in digital documents is at least as extensive and intimate as what was held on paper records at the Framing, and probably much more so. *See* Mary Czerwinski et al., Digital Memories in an Era of Ubiquitous Computing and Abundant Storage, Comm. of the ACM, Jan. 2006, at 45, available at http://goo.gl/einTJl. The storage of documents on media other than paper changes nothing about their Fourth Amendment significance. The same information about each American's life that once resided on paper and similar media in attics, garages, workshops, bedrooms, sewing rooms, and desk drawers, cf. *Chimel v. California*, 395 U.S. 752, 754 (1969), now resides, digitized, in cell phones and other electronic devices, as well as uploaded to service providers.

Regardless of its other determinations here, this Court could aid Fourth Amendment administration by explicitly recognizing digital information as "papers and effects" whose security against unreasonable seizure is constitutionally

protected. The Fourth Amendment must extend to these media if this Court is to aid the Supreme Court in "assuring preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo*, 533 U.S. at 34; *see also Jones*, 565 U.S. at 950; *id*. at 958 (Alito, J., concurring).

B. Marlow's Contract with Sprint Gave Him Certain Property Rights in His Personal Information

Finding that digital files are papers/effects does not, of course, determine *whose* they are. The better understanding, using the law of property, is that the CSLI was, in relevant part, Marlow's. Property concepts quite naturally provide the best framework for administering the Fourth Amendment, as the categories it lists are items of property. It also uses the possessive pronoun "their," which draws a line around the items in which a person may assert a right against unreasonable seizure or search. If the CSLI were not his, Marlow would not have legal cause to complain about the government's seizure. But his arrangement with Sprint/Nextel gave him a property right in the data that the government seized.

That legal conclusion is not surprising, because the property status of data is often allocated by contract. Discovery in this case shows that Marlow maintained two cell phone numbers, (410) 979-3339 and (240) 723-8294, with service for both

provided by Sprint/Nextel ("Sprint").[2] Sprint provided services as governed by its Terms of Service and Privacy Policy. In exchange for Marlow's payments, Sprint agreed, among other things, to maintain Marlow's privacy in accord with its express policy. *See* Terms & Conditions, Sprint (last updated July 1, 2013), https://shop2.sprint.com/en/legal/os_general_terms_conditions_popup.shtml. That Privacy Policy, incorporated by reference into the agreement between Marlow and Nextel, *id.*, is very clear about how information shared with Sprint was to be maintained: "We do not share information that identifies you personally with third parties other than as follows: . . . . [to] comply with the law or respond to lawful requests or legal process." Sprint Corporation Privacy Policy, Sprint (last updated July 22, 2016), https://www.sprint.com/legal/privacy.html.

Marlow's agreement with Sprint allocated property rights among the parties in all personally identifiable information. The contract gave Marlow the right to exclude all others from this data, except as specifically permitted. CSLI being personally identifiable information, Marlow thus had a property interest in his CSLI—including, as most relevant here, the right to exclude others.

---

[2] Defense counsel has informed *amicus* that the (240) phone was owned by a friend or girlfriend, but this fact does not change the legal analysis. In *Jones*, the automobile the defendant drove was registered to his wife. The Court nevertheless found that he had "at least the property rights of a bailee." 132 S.Ct. at 949 fn. 2. A bailee has the right to exclude all except the bailor. Thus, the technical owner is of no legal import here where Marlow stood in the position of "at least" a bailee. *Id.*

This language and the bargain struck here—to maintain informational privacy absent "lawful" or "valid" process—is standard in telecom contracts. *Compare, e.g.*, *id.*, *with* AT&T Privacy Policy, AT&T (last updated July 24, 2015) ("Comply with [valid] court orders and other legal process"), https://www.att.com/gen/privacy-policy?pid=2506, *and* Full Privacy Policy, Verizon (last updated May 2016) ("to comply with valid legal process including subpoenas, court orders or search warrants, and as otherwise authorized by law; in cases involving danger of death or serious physical injury to any person or other emergencies"), http://www.verizon.com/about/privacy/full-privacy-policy.

Like millions of cell phone users, Marlow provided consideration for the maintenance of privacy in his CSLI absent a "lawful request" compelling disclosure to a third party—that is, a valid legal process. In the absence of a "lawful request," the information was not Sprint's to give to the government.

Another conceptual approach is to treat such materials as within "personal curtilage." *See generally* Andrew Guthrie Ferguson, *Personal Curtilage: Fourth Amendment Security in Public*, 55 Wm. & Mary L. Rev. 1283 (2014). When people's digital items produce personal data, that data may be part of a "digital curtilage." Ferguson, *The Internet of Things*, *supra*, at 105. But a more precise and conventional legal framework for assessing this data is based on ownership status.

Awareness of common-law and contractual rights in information and data is still underdeveloped, and Fourth Amendment analysis suffers for it. This is in part because most enforcement of privacy policies comes through public enforcement actions, which result in settlement agreements with the Federal Trade Commission rather than reported court cases apportioning individual damages. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 585-586 (2014). But the FTC is enforcing contracts when it presses companies to adhere to their privacy and data-security promises. There would be a sharp dichotomy in federal treatment of privacy policies if this Court were to treat them as hortatory surplusage while the agency charged with policing deceptive trade practices treats them as entirely enforceable commitments.

The terminology that Congress has used in legislation illustrates the general understanding that communications data are property. Section 702 of the Telecommunications Act of 1996, for example, 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). The statute defines "Customer Proprietary Network Information" ("CPNI"), as "information that relates to the quantity, technical configuration, type, destination, 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…." *Id.* § 222(f)(1).

Congress used the adjective "proprietary" because it conceived of the data and information that telephone companies amass essentially as property. Doing so accords with communications' being the subject of contract terms, and it does not exclude the same information from being jointly owned by the customer. Indeed, the statute allocates some narrow property rights in CPNI to telecom customers. Consumers can require telecom providers to disclose copies of their CPNI to them, *Id.* § 222(c)(2), meaning the information is also theirs to possess and use if they want it. The statute's privacy requirements can be avoided "with the approval of the customer," *Id.* § 222(c)(1), meaning that customers' rights to exclude others from personal information and data are alienable, as property rights are.

There is an argument, if slightly glib, that Marlow's agreement with Sprint entitled him to any process established by a law. According to this argument, any legislation regularizing the sharing of information would be "lawful" or "a legal process," without regard to its standards. That interpretation is incorrect because it would render the contractual provision meaningless. It would not provide telecom consumers any benefit, and it could be excised without affecting the bargain. The appearance of the relevant text in the Privacy Policy suggests that it was meant to provide mobile users some measure of privacy.

The measure of protection a telecom privacy policy provides is more difficult to assess, but there are good reasons to treat the low "relevance" standard in § 2703(d) as insufficient. One is that its application is not limited to suspects but may allow the gathering of any user's data. The requirement of "specific and articulable facts" harkens to *Terry v. Ohio*, 392 U.S. 1 (1968), and it invites comparison between gathering of CSLI and the "stop-and-frisk" approved in *Terry*. That is a bit like "judging whether a particular line is longer than a particular rock is heavy," *Bendix Autolite Corp. v. Midwesco Enters.*, 486 U.S. 888, 897 (1988) (Scalia, J., concurring), but it can be done in rough fashion: *Terry* stops are restricted to suspects, where § 2703(d) orders are not. *Terry* stops announce themselves in real time—allowing the people detained to object—while § 2703(d) orders can be delayed, depriving subjects of the ability to timely object. A *Terry* stop likely produces a sense of subjugation, ignominy, and embarrassment—feelings that may dissipate in relatively short order—but a § 2703(d) order, once revealed can produce similar feelings of being watched, haunted, or objectified through data. Such an order also puts the data-subject at risk of embarrassing, disquieting, and invasive uses for an indefinite time after the search. That risk in particular counsels against treating data seizures as analogous to *Terry* stops.

Indeed, § 2703(d) does not include any limits on data retention or later use. Law-enforcement and national-security data-retention policies can be very long.

See, e.g., U.S. Dep't of Homeland Security, Privacy Impact Assessment for the Automated Biometric Identification System (IDENT) (2012), available at http://goo.gl/NFmz23 (records maintained for 75 years). The uses that will be made of data collected under § 2703(d) in the future are unknown, though they can be expected to grow as additional collection and processing technologies develop. The Association for Computing Machinery's special interest group on knowledge discovery and data mining ("SIGKDD") is but one locus of activity where data-mining technology is advancing. *See* About, SIGKDD (last visited Aug. 24, 2016), http://www.kdd.org/about. Acute challenges around data security mean that data collected under a § 2703(d) order is at risk of breach and acquisition by criminals and governments hostile to U.S. interests. See Office of Personnel Management, Cybersecurity Resource Center: Cybersecurity Incidents OPM.gov (last visited Aug. 24, 2016), available at https://www.opm.gov/cybersecurity/cybersecurity-incidents; Ellen Nakashima, *Powerful NSA Hacking Tools Have Been Revealed Online*, Wash. Post (Aug. 16, 2016), http://goo.gl/blJHyB. Unlike a *Terry* stop—whose consequences essentially end with its conclusion—data collection under § 2703(d) produces risks that may expand in unknown ways over long time periods.

Given the indeterminacy of the threats produced by data collections of this type, it is impossible to know whether retrospective relief for harms will be available. These open-ended risks particularly counsel interpreting the contract

between communications users and providers as giving users their full rights and not the permissive "stop and frisk"-like standard of § 2703(d).

In *Jones*, the Supreme Court used orthodox property law to administer the Fourth Amendment. It found that Jones was a bailee of his wife's car during the government's tracking of it. 132 S.Ct. at 949 fn. 2. That made the car "his" for Fourth Amendment purposes. Applying similar common-law property and contract rules now makes clear that the seized CSLI was, in relevant part, Marlow's. Specifically, Marlow had the right to exclude others from the personal information his use of his phones produced, and the exception required a higher showing than that found in § 2703(d). *Jones* is the most important precedent because it shows that the Supreme Court is setting aside the "reasonable expectation of privacy" test. *Jones* has laid the foundation for sounder Fourth Amendment administration.

C. *Jones* Reestablished Property as a Framework for Administering the Fourth Amendment, Including Non-Possessory Property Rights Such as the Right to Exclude Others

The Fourth Amendment lists four types of property—"persons, houses, papers, and effects"—in which people enjoy protection against unreasonable searches and seizures. Oddly and with difficulty, commentators and courts in the last four decades have often tried to administer this provision without reference to property through "privacy" and society's expectations around that malleable concept. But the Supreme Court's decision in *Jones* helped reset the focus on

property rights. 132 S.Ct. at 945. It is part of a line of recent cases that have eschewed the "reasonable expectation of privacy" test, including *Kyllo*, 533 U.S. at 27, *Florida v. Jardines*, 133 S.Ct. 1409, 1416 (2013), and *Riley*, 134 S.Ct. at 2473.

Jones is not as clear as it could be, but when the government "physically occupied private property for the purpose of obtaining information" without a warrant, that violated the Fourth Amendment. 132 S.Ct. at 949. The *Jones* Court characterized the totality of government activity as a "search," but the starting point was the invasion of a property right—the seizure that occurred when government agents placed the GPS device on Jones's car and used the car to transport their device. The Second Circuit characterized what happened in *Jones* as a "a technical trespass on the defendant's vehicle," *ACLU v. Clapper*, 785 F.3d 787, 823 (2d Cir. 2015), and that is correct in the main. It is not the trespass cause of action, of course, but basic property-law concepts that make sense of *Jones*.

The government did not take possession of the defendant's car, but by attaching its GPS device, it used the car to transport its sensor. The government's agents enjoyed the benefits of Jones's vehicle, taking use and enjoyment without a legal right to do so, and they deprived Jones of his right to exclude others. These seizures all underlaid their continuous, four-week search for Jones's location.[3]

---

[3] *Jones* repudiated the Seventh Circuit's *U.S. v. Garcia* opinion, where Judge Posner called "untenable" the idea that attaching a tracking device is a seizure. 474

Modern precision requires recognizing seizures when government agents violate any incident of property ownership, including the right to exclude others. The right to use and the right to the income of property—the enjoyment of its benefits—are examples of what law students are taught to be part of the "bundle of sticks" that comprises property rights. *See* A.M. Honoré, Ownership, in *Oxford Essays on Jurisprudence* 104-147 (A.G. Guest, ed. 1961).

A number of substantial authorities emphasize the importance of the right to exclude others as the essence of property. Blackstone defined property as "that sole and despotic dominion . . . exercise[d] over the external things . . . in total exclusion of the right of any other." 2 William Blackstone, Commentaries *2. The Supreme Court, too, has focused on exclusion as the critical property right. In *Loretto v. Teleprompter Manhattan CATV Corp*., 458 U.S. 419, 435 (1982), the Court called the right to exclude "one of the most treasured strands" of the property rights bundle. And in *Kaiser Aetna v. United States*, the Court explicitly called exclusion "one of the most essential sticks." 444 U.S. 164, 176 (1979).

The Supreme Court has sometimes wandered away from the full correlation between property rights and seizure that sound administration of the Fourth Amendment requires. Casual use of language in a spate of cases from the 1980s

---

F.3d 994, 996 (2007). The challenge of administering the Fourth Amendment as to data may require seemingly untenable positions to be made tenable.

suggests that only the right of possession—the "possessory" interest in property—is relevant to Fourth Amendment analysis. In *United States v. Place*, for example, the Court discussed the "possessory" interest in luggage. 462 U.S. 696, 705 (1983). In *United States v. Jacobsen*, it found a seizure because destruction of powder infringed "possessory interests." 446 U.S. 109, 113 (1984). In *United States v. Karo*, the Court found that installation of a beeper did not interfere with a "possessory" interest in a canister. 468 U.S. 705, 712 (1984). And in *Arizona v. Hicks*, it found that recording serial numbers from stereo equipment overturned for that purpose was not a seizure because it did not "'meaningfully interfere' with respondent's possessory interest in either the serial numbers or the equipment." 480 U.S. 321, 324 (1987) (citing *Maryland v. Macon*, 472 U.S. 463, 469 (1985)).

Justice Stevens's dissent in *Karo*, the beeper case, was correct, if muddy on property-rights distinctions: "Surely such an invasion is an 'interference' with possessory rights; the right to exclude . . . had been infringed." *Karo*, 468 U.S. at 729 (Stevens, J., dissenting). Justice Stevens wrote more clearly about seizure for the majority in *Horton v. California*: "[A] seizure deprives the individual of dominion over his or her person or property." 496 U.S. 128, 133 (1990).

In *Jones*, the government invaded the defendant's right to exclude others from his car. Here, the government invaded the defendant's right to exclude others

from his data. Invading non-possessory property interests can undercut the security that the Fourth Amendment is meant to guarantee as much as taking possession.

If Marlow's contract with Sprint gave him no property rights in the subject data and no constitutional claim to protection, the same would be true for millions of customers who seek to control access to information about themselves by contract. Privacy policies across the commercial world would have the status of loosely deceptive advertising. In communications, financial services, healthcare, and indeed every realm where contracts governing information are privately negotiated, privacy policies would be weakened. *See, e.g.*, Gramm-Leach-Bliley Act, Pub.L. 106–102, 113 Stat. 1338, at tit. V, subtit. A (Nov. 12, 1999) (codified at 15 U.S.C. §§ 6801-6809); Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub.L. 104–191, 110 Stat. 1936, at tit. II, subtit. F, §§ 261–264 (Aug. 21, 1996) (codified at 42 U.S.C. § 300gg; 29 U.S.C § 1181 *et seq.*; 42 USC 1320d *et seq.*); *see also* "Privacy of Consumer Financial Information," 65 Fed. Reg. 35162 (June 1, 2000); "Standards for Privacy of Individually Identifiable Health Information; Final Rule," 65 Fed. Reg. 82461 (Dec. 28, 2000).

The seizure of the CSLI took something of Marlow's, and it should trigger scrutiny for constitutional reasonableness just as the seizure of the car did in *Jones*.

D. Under *Katz*, Having a Contract-Based Property Right in Personal Information Also Triggers Fourth Amendment Protection

Part of the challenge in administering the Fourth Amendment as to data has been the "reasonable expectation of privacy" test devised by Justice Harlan in his solo concurrence in *Katz*, 389 U.S. at 361 (Harlan, J., concurring). But the majority opinion in *Katz*, written by Justice Stewart, rested on the physical protection the defendant had given to his oral communications—going into a phone booth—not on subjective expectations of privacy, let alone whether those expectations were reasonable. *Id.* at 352. The *Katz* majority treated Fourth Amendment protection as turning on the physical and legal conditions governing access to information.

The lines Justice Stewart used to reverse *Olmstead v. United States*, 277 U.S. 438 (1928), remind us of *Katz*'s actual holding and rationale:

> What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.

Id. (citations omitted).

This language is not a crystal-clear rule for determining what is protected and what is not, but the better reading is that "may" in the latter sentence indicates possibility, that constitutional protection of Katz's conversation turns on some contingency. But what contingency? The most apt interpretation is right there in the sentence: whether something is "preserve[d] as private." *Id.*

Katz sought to preserve the privacy of his phone conversation by entering into a phone booth, which is designed with sound-baffling qualities, and he succeeded. With that condition cleared up, the final sentence in the block-quote above comes to mean, "what he preserved as private is constitutionally protected." Ordinary husbandry of information—the specific information at issue being the sound of his voice—gave Katz privacy and in turn Fourth Amendment protection. *Cf. Ex Parte Jackson*, 96 U.S. 727, 733 (1878) ("Letters and sealed packages . . . in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles. The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be.").

Here, Marlow contracted with a telecom provider to "not share information that identifies you personally with third parties." Having sought to make private the documentation of his whereabouts that is essential for the provision of that service, Marlow is entitled to constitutional protection, as are all telecom users.

Integrating the Fourth Amendment with modern communications was challenging enough before later judicial opinions and popular reinterpretations treated *Katz* as breaking the link between property and Fourth Amendments interests. But the foray into administering the Fourth Amendment via

"expectations" arose from one justice's lone concurrence. The *Katz* majority did not reject the Fourth Amendment's grounding in property law. Rather, it more subtly examined the physical and legal relationships between individuals and the things with which they interact to determine when the government has invaded the protections of the Fourth Amendment. Indeed, *Katz*'s majority opinion affirms property interests as a hallmark of the Fourth Amendment by examining what the individual "seeks to control" through various physical and legal arrangements.

Giving consideration in exchange for the promise to hold information privately is demonstrably "seeking to preserve what is private" per *Katz*. As much as a person can erect a wall around a telephone booth to maintain informational privacy, he or she may erect a contractual wall to accomplish the same through property rights. Indeed, bargained-for maintenance of privacy is the foundation to many business and imitate relationships, including the attorney-client one. *See, e.g.*, *Olmstead*, 277 U.S. at 487 (Butler, J., dissenting).

The *Katz* majority's reasoning easily disposes of the question whether seizing Marlow's data required a warrant. Marlow had agreed to pay Sprint for—among other things—keeping his CSLI secure from prying eyes except to comply with "lawful process" meeting a high standard. The contract thus generated a *bona fide* property right, the violation of which triggers scrutiny for reasonability. And the general rule is that seizure in such circumstances requires a warrant.

II. THE GOVERNMENT SEIZED MARLOW'S CSLI WITHOUT THE WARRANT REQUIRED BY THE FOURTH AMENDMENT

The Supreme Court has long held that the government may neither seize nor search property without first acquiring a warrant, upon probable cause. "Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, . . . reasonableness generally requires the obtaining of a judicial warrant." *Vernonia School Dist. 47J v. Acton*, 515 U. S. 646, 653 (1995). In fact, "[i]n the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement." *Riley*, 134 S.Ct. at 2582 (citing *Kentucky v. King*, 563 U.S. 452, 459-61 (2011)).

As noted above, the contract between Marlow and Sprint gave Marlow the right to exclude others from his CSLI. Marlow's CSLI was obtained by court order under § 2703(d) of the SCA, which does not require the sufficiency of evidence that a probable cause warrant requires. *Compare* 18 U.S.C. § 2703(c)(1), *with id.* § 2703(d). But to avoid the warrant requirement, § 2703(d) must fall under an existing exception. Otherwise, it is not a "valid" or "lawful" process that voids Marlow's right to exclude. No exception to the warrant requirement applies to the seizure of Marlow's CSLI: There was no hot pursuit, inventory search, emergency aid, or exigent circumstance. The data was held by the telecom provider, and a preservation order under §2703(f) would not have violated Marlow's right to exclude others.

In sum, the government was pursuing an orderly, months-long investigation. It would have imposed no great burden on law enforcement to make an application for a probable-cause warrant under § 2703(c)(1). Accordingly, the seizure of Marlow's CSLI was an unconstitutional seizure under the Fourth Amendment.

III. THE THIRD-PARTY DOCTRINE PROVIDES NO RELIEF TO THE GOVERNMENT

The court below permitted a § 2703(d) order under the third-party doctrine, which says that a person has no Fourth Amendment interest in information they share with a third party. *See, e.g.*, *Smith v. Maryland*, 442 U.S. 735 (1979); *United States v. Miller*, 425 U.S. 435, 443 (1976). But this doctrine is not a freestanding constitutional directive, instead having developed as an offshoot of the "reasonable expectation of privacy" test. *Smith*, 442 U.S. at 780-46; *see also Katz*, 389 U.S. at 361-62 (Harlan, J., concurring). That formulation has certainly enjoyed repetition, but it was not the holding in the case. *Katz* would have come out the same way regardless of how Justice Harlan voted or what he wrote, so his solo writing does not supply the legal principle on which the *Katz* case turned.

Tellingly, in the Supreme Court's most recent precedents, justices who don't always agree in this area have backed away from Justice Harlan's test and its progeny. The third-party doctrine is thus on ground even shakier than the "reasonable expectation of privacy" test. In the Court's most important relevant cases—*Kyllo*, *Jones*, *Jardines*, and *Riley*—the Court notably chose not to rely on

the "reasonable expectation" test, turning instead at least in part to property-based analyses. *See Riley*, 134 S.Ct. at 2478, 2485 (using property-rights analysis to determine if a cell phone was searchable incident to arrest); *Jardines*, 133 S.Ct. at 1414 (relying in part on property rights); *Jones*, 132 S.Ct. at 954 (expressly not applying *Katz* where property-based reasoning sufficed); *Kyllo*, 533 U.S. at 27 (no application of "reasonable expectations" analysis).

Note well the dog that did not bark in *Riley*. The *Riley* Court did not consider that contacts and pictures in today's phones are often conveyed to cloud storage and communications providers. *See Riley*, 134 S.Ct. at 2480-81. Under "reasonable expectations," the third-party doctrine may apply and such voluntary disclosures would denude phone data of any privacy interest. But the Court was not applying the "reasonable expectation of privacy" test, so there was no third-party doctrine to consider either. The Court found that there were significant privacy interests—including such interests in location information—without respect to whether third parties were involved in providing services or storing data. *Id*. at 2487-92; *see also Jones*, 132 S.Ct. at 957 (Sotomayor, J., concurring).

Quite plainly, the third-party doctrine is in decline. Circuit courts have repeatedly cut back on its application. *See, e.g.*, *Dov v. Broderick*, 225 F.3d 440, 450-52 (4th Cir. 2000) (doctrine does not apply to patient records held by medical case provider); *DeMassa v. Nunez*, 770 F.2d 1505, 1508 (9th Cir. 1985) (doctrine

does not apply to attorney-client communications). Application of the third-party doctrine to data shared between a user and provider would open up huge troves of information for perusal by government agents without a probable-cause warrant.

Justice Sotomayor questioned the third-party doctrine trenchantly in her *Jones* concurrence, an opinion worth quoting at some length:

> 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. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers . . . . I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. 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. See *Smith*, 442 U.S., at 749, 99 S.Ct. 2577, 61 L. Ed. 2d 220 (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes"); see also *Katz*, 389 U.S., at 351-352, 88 S.Ct. 507, 19 L. Ed. 2d 576 ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected").

Jones, 132 S.Ct. at 957 (Sotomayor, J., concurring). Justice Sotomayor is correct: application of the third party doctrine to digital information is fraught with danger. The quantum of information that a person's telecom records can reveal in the

smartphone era is just as invasive as a search of a home computer—or an entire home in 1789. *See Riley*, 134 S.Ct. at 2489-90.

Marlow paid Sprint for protection of his privacy—the right to exclude people from personal information except in cases where there is a valid legal process. The lower court's decision to apply the third party doctrine and allow the § 2703(d) court order is contrary to the Supreme Court's relatively clear signaling about the gathering of data via digital devices and services: get a warrant.

CONCLUSION

It is no small challenge to apply the Fourth Amendment in this era of digital devices. Resorting to time-honored legal principles such as property and contract can help ground courts' analyses much more firmly than the fading "reasonable expectations" doctrine. Because Marlow enjoyed the right to exclude others from his private information—a right acquired by contract—it was unreasonable to seize the data without a warrant. Accordingly, this Court should reverse the court below.

Respectfully submitted this 26th day of August, 2016,

Ilya Shapiro
Counsel of Record
Jim Harper*
Randal J. Meyer*
CATO INSTITUTE
1000 Mass. Ave., N.W.
Washington, D.C. 20001
(202) 842-0200
ishapiro@cato.org
*Admission pending

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because it contains 6,265 words, excluding the parts exempted by Fed. R. App. P. 32(a)(7)(B)(iii) and D.C. Cir. Rule 32(a)1.
2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word 2013 in Times New Roman, 14 point font.

/s/Ilya Shapiro
Ilya Shapiro
Counsel for *Amicus Curiae*

CERTIFICATE OF SERVICE

I hereby certify that, on August 26, 2016, I filed the foregoing brief with this Court by causing a true digital copy to be electronically uploaded to the Court's CM/ECF system and by causing nine true and correct copies to be delivered by FedEx next business day delivery to the Court. Service was accomplished by the CM/ECF system on the following counsel, who are registered CM/ECF users:

Daniel Joseph Lenerz
Elizabeth Trosman
Lori Buckler
U.S. Attorney's Office
(USA) Appellate Division
555 4th Street, NW
Washington, DC 20530
(202) 252-6829
daniel.lenerz@usdoj.gov
elizabeth.trosman@usdoj.gov
Lori.Buckler@usdoj.gov

Matthew G. Kaiser
KaiserDillon PLLC
1401 K Street NW Suite 600
Washington, DC 20005
(202) 640-2849 (direct)
(202) 640-2850 (main)
mkaiser@kaiserdillon.com

Stephen Scavuzzo
Law Office of Stephen Scavuzzo
8200 Greensboro Drive Suite 900
McLean, VA 22101
(703) 319 8770 ·
Fax: (703) 319 1747 ·
scavuzzolaw@aol.com

Deborah A. Persico
Deborah A. Persico, PLLC
5614 Connecticut Ave. NW Suite 105
Washington, DC 20015
(202) 244-7127
persico33@yahoo.com

/s/Ilya Shapiro
Ilya Shapiro
Counsel for *Amicus Curiae*