No. 16-402

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Sixth Circuit

BRIEF FOR THE COMPETITIVE ENTERPRISE INSTITUTE, CATO INSTITUTE, REASON FOUNDATION, AND COMMITTEE FOR JUSTICE AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

Ilya Shapiro
CATO INSTITUTE
1000 Mass. Ave. N.W.
Washington, D.C. 20001
(202) 842-0200
ishapiro@cato.org

Manuel S. Klausner
LAW OFFICES OF MANUEL S. KLAUSNER
One Bunker Hill Building
601 W. Fifth St., Suite 800
Los Angeles, CA 90071
(213) 617-0414
mklausner@klausnerlaw.us

Jim Harper
Counsel of Record
Ryan C. Radia
COMPETITIVE ENTERPRISE INSTITUTE
1310 L St. NW, 7th Floor
Washington, D.C. 20005
(202) 331-1010
jim.harper@cei.org

Curt Levey
The Committee for Justice
722 12th St. NW, 4th Floor
Washington, DC 20005
(202) 270-7748
clevey@committeeforjustice.org

August 11, 2017

QUESTION PRESENTED

Can the government seize and review anyone's cell-site location data—which reveals all of their movements over extended periods—without a warrant?

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Statutes

Other Authorities

INTEREST OF *AMICI CURIAE*[1]

Founded in 1984, the **Competitive Enterprise Institute** ("CEI") is a non-profit public policy organization dedicated to advancing the principles of limited government, free enterprise, and individual liberty. CEI frequently publishes research and commentary on topics at the intersection of property rights, markets, free enterprise, and liberty. The instant case concerns CEI because proper administration of the Fourth Amendment would allow businesses to protect their customers' privacy consistent with their interests as determined in the marketplace.

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. Cato's Center for Constitutional Studies promotes the principles of limited constitutional government that are the foundation of liberty. To those ends, Cato publishes books and studies, conducts conferences, produces the annual *Cato Supreme Court Review*, and files *amicus* briefs. The present case centrally concerns Cato because it represents an opportunity to improve Fourth Amendment doctrine and maintain that provision's protections in the modern era.

Reason Foundation is a nonpartisan and nonprofit public policy think tank founded in 1978. Reason's mission is to advance a free society by developing, applying, and promoting libertarian principles and policies—including free markets, individual liberty,

---

[1] All parties lodged blanket consents with the Clerk. No counsel for any party authored this brief in whole or in part and no person or entity other than *amici* funded its preparation or submission.

and the rule of law. Reason supports dynamic market-based public policies that allow and encourage individuals and voluntary institutions to flourish. Reason advances its mission by publishing Reason magazine, as well as commentary on its websites, www.reason.com, reason.org, and www.reason.tv. To further Reason's commitment to "Free Minds and Free Markets," Reason selectively participates as *amicus curiae* in cases raising significant constitutional issues.

Founded in 2002, the **Committee for Justice** (CFJ) is a nonprofit, nonpartisan organization dedicated to promoting the rule of law, including the Constitution's limits on the power of government and its protections of individual liberty, including the Fourth Amendment right to be free from unreasonable searches and seizures. CFJ is particularly concerned with the threat to these protections posed by a misfit between existing law—in this case, the "reasonable expectation of privacy" test and the third-party doctrine—and rapid technological advances.

INTRODUCTION AND SUMMARY OF ARGUMENT

For nearly 40 years,[2] this Court and courts below have struggled with using a sociological method for interpreting the Fourth Amendment in difficult cases. They have asked whether government agents disturbed a "reasonable expectation of privacy," reasoning backward from the answer to whether or not a "search" offensive to the Constitution has occurred.

That methodology has been difficult for courts to apply consistently, and in recent years this Court has

---

[2] *Katz v. United States*, 389 U.S. 347 (1967), was decided on December 18, 1967.

used it less and less often as a decision rule. This Court should shed that sociological approach and adopt a juridical method for applying the Fourth Amendment. It should assess the facts of the case in terms of the law, encouraging lower courts to do the same.

Specifically, the Court should examine the following questions:

- Was there a search?
- Was there a seizure?
- Was any search or seizure of "persons, houses, papers, [or] effects"?
- Was any such search or seizure reasonable?

Using that simple and familiar legal methodology would allow this Court to address directly the challenging questions this case presents, including: When does a seizure of data occur? When does a search of data occur? When is data a constitutional "paper" or "effect"? Who has property rights in data sufficient to assert Fourth Amendment rights in it?

The government's compulsory acquisition of data in this case was a seizure. Processing the data to make it human-readable was a search. The records were in relevant part the property of Messrs. Carpenter and Sanders, who enjoyed contractual rights and regulatory protections making them so. And digital documents are best treated as constitutional "papers" or "effects."

That leaves the question whether it was reasonable for the government to seize and search them. There is a presumption in favor of the warrant requirement suggested by the text of the Fourth Amendment, and it is confirmed by this Court's precedents. Thus, it was

unreasonable to seize and search the data without a warrant. Lacking exigency or other excuse, the government should have gotten one.

The interests of Messrs. Carpenter and Sanders are not paramount to *amici*, of course. But as the importance of digital communications and data grows in society, the imperative to straightforwardly address their legal and constitutional status rises.

Without breaking from precedents, this Court can revise Fourth Amendment practice and determine when and how communications and data fit into the Fourth Amendment's categories of protected things. Doing so would permit courts below to address seizures and searches of communications and data forthrightly, confidently assessing the reasonableness of such government action. Here, the result of that analysis calls for the Court to find in favor of the petitioner.

ARGUMENT

I. THIS COURT SHOULD APPLY THE TERMS OF THE FOURTH AMENDMENT IN ALL FOURTH AMENDMENT CASES

The first phrase of the Fourth Amendment says, "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. Absent confusing doctrine, courts would analyze its elements as follows:

- Was there a search?
- Was there a seizure?
- Was any search or seizure of "persons, houses, papers, [or] effects"?

- Was any such search or seizure reasonable?

If there was a search or seizure, if it was of protected things, and if it was unreasonable, then the right has been violated. That is how to administer the Fourth Amendment.

In cases dealing with familiar objects, this Court applies the Fourth Amendment consistent with the language of the law. It looks for seizures and searches of defendants' protected items, then assesses whether or not they were reasonable. (Seizures often precede searches, so reversing the order in which the Fourth Amendment lists them is sensible.)

In *Terry v. Ohio*, 392 U.S. 1 (1968), for example, this Court applied the Fourth Amendment soundly, creating a lasting and useful precedent. The government had urged the Court to place brief "stop and frisk" incidents like a pat-down outside the scope of the Fourth Amendment, *id*. at 16 n.12., arguing that police behavior short of a "technical arrest" or a "full blown-search" did not implicate constitutional scrutiny. *Id*. at 19. This Court rejected the idea that there should be a fuzzy line dividing "stop and frisk" from "search and seizure."

Instead, this Court wrote with granular precision about the seizure, then the search, of Terry: "[T]here can be no question . . . that Officer McFadden 'seized' petitioner and subjected him to a 'search' when he took hold of him and patted down the outer surfaces of his clothing." *Id*. One following the other, the seizure and search were reasonable and therefore constitutional.

Justice Douglas dissented from the ruling but agreed that Terry was "seized" within the meaning of

the Fourth Amendment. *Id.* at 35 (Douglas, J., dissenting). "I also agree," he wrote, "that frisking petitioner and his companions for guns was a 'search.'" *Id.*

Terry and its progeny demonstrated their value again in the recent *Riley v. California* decision, 134 S. Ct. 2473 (2014). Numerous seizures and searches of familiar objects like cars and people were administered using direct application of the Fourth Amendment's terms rather than odd and derived doctrine.

In *Riley*, Officer Charles Dunnigan pulled David Riley over, seizing him and his car consistent with the application of the Fourth Amendment to traffic stops in *Brendlin v. California*. 551 U.S. 249, 254–63 (2007). Upon learning that Riley was driving with a suspended driver's license, Officer Dunnigan removed him from the car, continuing the original seizure of Riley with an additional legal basis for doing so: reasonable suspicion of another violation.

Officer Ruggiero prepared the car for impoundment, a further seizure, consistent with a policy that prevents suspended drivers from returning to, and continuing to operate, their vehicles. He began an "impound inventory search" of the car, as approved in *South Dakota v. Opperman*. 428 U.S. 364, 376 (1976).

That search turned up guns in the engine compartment of the car, so Officer Dunnigan placed Riley under arrest, continuing the ongoing seizure of Riley's body under new legal authority. Officer Dunnigan conducted a search incident to arrest—permitted to aid in the discovery of weapons or of evidence that suspects might destroy. *Chimel v. California*, 395 U.S. 752, 762–63 (1969). Consistent with standard practice for a "booking search," yet another legal basis for both

searching suspects and seizing their property, *see, e.g.*, *Illinois v. Lafayette*, 462 U.S. 640 (1983), Officer Dunnigan examined Riley's person and seized his possessions, including his cell phone.

All these steps were dogs that didn't bark—government actions unchallenged or fully disposed of in courts below. That is because this Court has given law enforcement and courts the legal tools to dispose of them: identify when seizures and searches of protected things have occurred, then determine whether or not they are reasonable.

Courts are well-equipped to make those legal and fact-specific judgments. If the constitutionality of all these investigatory steps turned on sociological questions such as whether government agents had defeated a society-wide "reasonable expectation of privacy," this Court would have a full docket indeed.

Happily, *the Riley* opinion also assessed the search of the phone as the search that it was, without respect to privacy expectations. Having found that the phone was searched in the absence of exigency, this Court laid down the general rule so strongly implied by the second half of the Fourth Amendment: "get a warrant." 134 S. Ct. at 2495.

This case is not *Riley*. It involves both a seizure of data unconnected to a physical effect and a search of that data. A central question is what rights in the data were seized, and whose they were. The status of data as a "paper" or "effect" needs clearing up, too.

But the Court does not need to retreat to doctrine when communications and data are at issue. Data can be seized under the Fourth Amendment just like people and cars. Data can be searched just like homes.

Treating data consistently with physical items would focus courts on the key Fourth Amendment question: whether given seizures or searches are reasonable. Confusing doctrine stands in the way of their doing so.

II. THIS COURT SHOULD ESCHEW THE UNSOUND "REASONABLE EXPECTATION OF PRIVACY" TEST AND OTHER UNHELPFUL DOCTRINES

Relying on doctrine, the decision below begins by noting an alleged constitutional distinction between communications content and routing information. "In Fourth Amendment cases the Supreme Court has long recognized a distinction between the content of a communication and the information necessary to convey it." J.A. 61-2. An uninitiated lawyer or ordinary American would have difficulty understanding what this has to do with constitutional protection for "persons, houses, papers, and effects," which makes no such distinction.

The court below began as it did because this Court has often fallen back on confusing doctrine when applying the Fourth Amendment in hard cases. But this Court can apply the terms of the Fourth Amendment to communications and data cases in a granular way, as it has in the past.

A line of opinions extending from *Ex Parte Jackson*, 96 U.S. 727 (1878), through Justice Butler's dissent in *Olmstead v. United States*, 277 U.S. 438 (1928), and the majority opinion in *Katz v. United States*, 389 U.S. 347 (1967), shows how to integrate communications and data with the Fourth Amendment's textual frame-

work. But a detour over the last forty years into "reasonable expectations" doctrine has undercut sound administration of the Fourth Amendment.

A. *Ex Parte Jackson* Properly Protected Communications in Transit by Protecting Papers and Effects as Such

This Court correctly applied the Fourth Amendment to communications in *Ex Parte Jackson*, 96 U.S. 727 (1878). The opinion did not state in bullet-point order that the postal mail in question, having been handed over to the government, was a) searched, b) a paper or effect, and c) unreasonably searched without a warrant. But it held that "[l]etters 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." *Id*. at 733.

Mailed items remain the papers and effects of their owners while in transit, even though they are not in the possession of their owners. Accessing their contents, such as by opening envelopes, unfolding papers and such, is a search. Doing those things requires a warrant.

The outward form and weight of such items, not being sealed from inspection, are not constitutionally protected. This was early acknowledgement of the difference between what we now call "plain view" and what might be called "plain concealment." It takes no search to discover what is in plain view, so the Fourth Amendment is not implicated. *See Horton v. California*, 496 U.S. 128 (1990). It takes a search to reveal concealed matter, so the Fourth Amendment pertains. The issues are put in play by constitutional text and

disposed of using physics and law, not privacy expectations. *See* Jim Harper, *Escaping Fourth Amendment Doctrine After* Jones*: Physics, Law, and Privacy Protection*, 2011–2012 Cato Sup. Ct. Rev. 219 (2012).

Here, the court below, thrown off by more recent doctrine, treated *Jackson* as a special rule about communications. J.A. 61-6. But *Jackson* simply applied common sense: exposed facts do not require a search to be discovered, even when they are facts about papers and effects. Under *Jackson*, communications written on the outside of an envelope would not be protected, because *Jackson* did not create a content/non-content distinction.

In the 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 (2003). This Court would face that technology after the passage of some time, but perhaps 1928 was too soon because the Court did not soundly address the parallels between postal and telephonic communications in *Olmstead*.

B. *Olmstead* Involved Seizures and Searches of a Wire and Electronic Papers/Effects

Fifty years after *Jackson*, *Olmstead v. United States*, 277 U.S. 438 (1928), incoherently declared wiretapping "the use of the sense of hearing, and that only." *Id*. at 464. A telephone communication renders sounds as electronic signals that travel invisibly and inaudibly along a wire, to be re-formed into audible sounds at the other end. Collecting those signals and reproducing them requires attachments, equipment, and processing well beyond simple hearing.

Justice Butler's dissent stands out because he followed the same sensible lines drawn in *Jackson*, even though the media were now wire and electrons instead of paper and ink. Though he left implicit the physical protections for these communications, Justice Butler identified the private law protections arrayed around telephonic communications. Seizure and search disrupted those arrangements when government agents wiretapped a telephone line: "The contracts between telephone companies and users contemplate the private use of the facilities employed in the service," he wrote. "The communications belong to the parties between whom they pass. During their transmission, the exclusive use of the wire belongs to the persons served by it." *Id.* at 487 (Butler, J., dissenting).

Government agents invaded property rights in the physical wire and in the communication running over it. Specifically, the government's use of the wire and copying of the electronic effects eviscerated Olmstead's right to exclude others from his property—a small but constitutionally significant seizure. The contemporaneous rendering of the communication signal into an audible sound was a search of it. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 551 (2005) ("[A] search occurs when information from or about the data is exposed to possible human observation."). The wiretap should have required a warrant.

It would have taken prescience indeed to recognize in the 1920s that telephonic and later digital communications would be the scions of physical mail. *But see Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting) ("Ways may someday be developed by which the Gov-

ernment, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.") Even now, the idea that papers and effects may take electronic or digital form takes some getting used to. But that ground is long since broken. The Court's treatment of a suitably shrouded oral communication as a constitutionally protected item in *Katz* has been widely accepted.

C. The *Katz* Majority Inarticulately Applied the Fourth Amendment's Terms to a Shrouded Oral Communication

Regrettably, when the Court reversed *Olmstead*, it avoided stating directly that the suitably concealed sound of a person's voice is a transitory "effect." (If the language of the Fourth Amendment applies, it almost certainly must be.) And even more unfortunately, the popular treatment of *Katz v. United States*, 389 U.S. 347 (1967), has been to ignore the majority's reasoning in favor of Justice Harlan's solo concurrence, which attempted to reframe Fourth Amendment jurisprudence around "reasonable expectations of privacy."

But the *Katz* majority decision was an inarticulate parallel to *Ex Parte Jackson*. The Court followed the same line as *Jackson* about disclosed matter requiring no search and concealed things requiring a seizure or search. "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.* at 351 (citations omitted).

The paragraphs that followed discussed the import of Katz's going into a phone booth made of glass, which concealed the sound of his voice. *Id*. at 352. Against the argument that Katz's body was in public for all to see, the Court wrote: "[W]hat he sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear." *Id*. The government's use of a secreted listening and recording device to enhance ordinary perception overcame the physical concealment Katz had given to his voice. Gathering the sound waves seized something of Katz's.

But in his solo concurrence, which was unnecessary to the outcome of the case, Justice Harlan shared his sense of how the Constitution controls government access to private communications: "My understanding," he wrote, "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.'" *Id*. at 361. Justice Harlan's understanding has not aided courts' administration of Fourth Amendment cases.

D. The Ills of the "Reasonable Expectation of Privacy" Test

Since *Katz*, courts have often followed Justice Harlan's concurrence, attempting to analyze whether defendants have had a "reasonable expectation of privacy" in information or things. Under Harlan's concurrence, but not the *Katz* majority's rationale, the existence and defeat of a "reasonable expectation of privacy" signals a constitutional search generally requiring a warrant.

Alas, courts rarely perform the full analysis. They infrequently inquire into a defendant's "actual (subjective) expectation of privacy," for example, or how it was "exhibited." *See* Orin Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. Chi. L. Rev. 113 (2015).

The second half of the test invites justices and judges to try to assess the entire society's emergent views on privacy. That is a sociological exercise, not a juridical one. It does not involve the application of law to facts or fact-specific judgments. It requires judges to use their own views or best estimations about the privacy interests of the whole society.

A particularly poor example of the test as applied is the opinion in *Smith v. Maryland*, 442 U.S. 735 (1979), in which Justice Blackmun walked through influences that would suppress expectations of privacy in phone-dialing information and none that would support it. *See id.* at 742–43. The court below here relied heavily on *Smith*, which in addition to being poorly reasoned may also be distinguished, given the great quantities of data at stake in cases like the present one.

The subjectivity of Justice Harlan's formulation is compounded by its essential circularity. Societal expectations guide judicial rulings, which guide societal expectations, and so on. That circularity is especially problematic here at the onset of the Information Age because digital communications and data are only beginning to take their place in society. Expectations about privacy in this medium are still taking form, and the technology continues to change, so there is simply no objectively reasonable sense of privacy for judges to discover.

E. Corollaries of the "Reasonable Expectation of Privacy" Test Are Even Worse

The "reasonable expectation of privacy" test has at least two corollaries that move doctrine even further from the Fourth Amendment's language and meaning. The first is the doctrine that treats searches tailored for illegal things as non-searches. The second is the "third-party doctrine," which denies that shared things can be unreasonably seized or searched.

Illinois v. Caballes, 543 U.S. 405 (2005), is typical of "reasonable expectation" cases in that it did not examine (or even assume) whether Roy Caballes had exhibited a subjective expectation of privacy in the trunk of his car when government agents subjected it to the ministrations of a drug-sniffing dog. Thus, the Court could not take the second step, examining its objective reasonableness.

Instead, the *Caballes* Court skipped forward to a corollary of the "reasonable expectations" test that the Court had drawn in *United States v. Jacobsen*, 466 U.S. 109 (1984): "Official conduct that does not 'compromise any legitimate interest in privacy' is not a search subject to the Fourth Amendment." *Caballes*, 543 U.S. at 408 (quoting *Jacobsen*, 466 U.S. at 123). Possession of drugs being illegal, there is no legitimate expectation of privacy in their possession. Thus, a search aimed at illegal drugs is not a search. That's confounding.

That entirely logical extension of "reasonable expectations" doctrine reveals the doctrine's role in delinking Fourth Amendment decisions from the Fourth Amendment's text. Now, instead of examining whether searches and seizures are reasonable, courts

applying the *Jacobsen*/*Caballes* corollary can uphold any activity of government agents that appears sufficiently tailored to discovering only crime. The most intensive government examination of persons, houses, papers, and effects can be "not a search," *id*., no matter how intimate it is, no matter how often it recurs, and irrespective of any context or circumstances.

The second corollary of "reasonable expectations" doctrine, more relevant here, similarly breaks the link between the terms of the law and outcomes in cases. That is the "third party doctrine," which the court below relied on here.

The Bank Secrecy Act ("BSA"), Pub. L. No. 91-508, 84 Stat. 1114 (codified as amended at 12 U.S.C. §§ 1951–59. (2000)) requires banks to maintain records and file reports with the Treasury Department if they "have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings." 12 U.S.C. § 1829b(a)(2) (2000). In *California Bankers Ass'n v. Shultz*, 416 U.S. 21 (1974), several parties challenged the BSA's requirements. The records-collection part of the law does not require disclosure to the government, so the Court found that it does not implicate the Fourth Amendment. *Id.* at 54. As to the reporting requirements, the Court denied standing to bank depositors who could not show that information about their financial transactions had been reported. *Id*. at 67–68.

Justice Thurgood Marshall criticized how the Court avoided finding that mandated record-keeping affects a constitutional seizure just because the government would acquire the records later. "By accepting the Government's bifurcated approach to the recordkeeping requirement and the acquisition of the records, the majority engages in a hollow charade whereby Fourth

Amendment claims are to be labeled premature until such time as they can be deemed too late." *Id.* at 97 (Marshall, J., dissenting).

Two years later, in *United States v. Miller*, 425 U.S. 435 (1976), the Court held that a defendant had no Fourth Amendment interest in records maintained about him pursuant to the BSA. *Id.* at 442–43. It did not examine whether the operation of the BSA was a seizure or search, but used "reasonable expectations" doctrine to dismiss Miller's Fourth Amendment interests in documents reflecting his financial activities. This was because they were held by a financial services provider: "we perceive no legitimate 'expectation of privacy' in their contents." *Id.* at 442.

Under these cases, the government can compel a service provider to maintain records about a customer and then collect those records without implicating his or her Fourth Amendment rights. *Cf. Los Angeles v. Patel*, 135 S. Ct. 2443 (2015) (holding requirement that hotel operators make their guest registries available to the police on demand facially unconstitutional). The rule of *Miller* appears to be that Americans forfeit their Fourth Amendment interests in any material that comes into possession of a third party. This at least elides subtler questions about who owns communications and data such as to enjoy a right to their protection from unreasonable seizure and search.

Based as they are in "reasonable expectations" doctrine, these holdings are hard to square with the Fourth Amendment's text. And they grow further out of synch with each step forward in modern, electronically connected living.

Incredibly deep reservoirs of information are constantly collected by third-party service providers today. Cellular telephone networks pinpoint customers' locations throughout the day through the movement of their phones. Internet service providers maintain copies of huge swaths of the information that crosses their networks tied to customer identifiers. Search engines maintain logs of searches that can be correlated to specific computers and the individuals that use them. Payment systems record each instance of commerce and the time and place it occurred. This trend will only accelerate as the "Internet of Things" supplies data revealing more and more of our activities—even use of our household appliances—to third-party service providers.

The totality of these records are very, very revealing of innocent people's lives. They are a window onto each individual's spirituality or religion, feelings, and intellect. They can reveal excruciatingly intimate details about physical and mental health, as well as marital and family relations. They reflect each American's beliefs, thoughts, emotions, sensations, and relationships. Their security ought to be protected from unreasonable seizure—as they are the modern iteration of our papers and effects. *See United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring). These items should generally not be seized without a warrant.

Thanks to recent cases, this Court is positioned to apply traditional common-law concepts such as property rights to digital communications and data, placing them within the framework set out by the text of the Fourth Amendment.

III. THIS COURT'S RECENT CASES ARE A FRAMEWORK FOR ADMINISTERING THE FOURTH AMENDMENT IN A RELIABLE AND JURIDICAL WAY

Familiar but circular and misleading doctrine like the "reasonable expectation of privacy" test does not square the Fourth Amendment's terms with the facts in particular cases. This Court's recent Fourth Amendment opinions, though, provide a framework for a clear return to adjudicating the Fourth Amendment as a law, even in difficult "high-tech" cases. *See* Jim Harper, *Administering the Fourth Amendment in the Digital Age*, Nat'l Const. Center, https://constitutioncenter.org/digital-privacy/The-Fourth-Amendment-in-the-Digital-Age. In all cases, the Court can follow the methodology suggested by the Fourth Amendment, which is to look for searches, look for seizures, determine whether they go to constitutionally protected items, and then determine whether they are reasonable.

This does not mean that the precise way to apply the Fourth Amendment's terms to communications and data is already obvious. It requires this Court to integrate advancing technology with long-standing legal principles. In doing so, this Court should find that data and digital communications are property that can be seized and searched even when the owners of the data are not in possession of it.

A. *Jones* Was a Seizure Case

Though this Court referred to what happened in *United States v. Jones*, 132 S. Ct. 945 (2012), as a "search," the precipitating constitutional invasion was a seizure. That seizure occurred when government agents attached a device to a car that was not theirs,

making use of it to transport their device without a warrant. *Id.* at 949; s*ee ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015) (referring to attachment of GPS device in *Jones* as "a technical trespass on the defendant's vehicle"). Though small, that seizure of Jones's car was real. It abrogated Jones's right to exclude and awarded the government a right to use the vehicle for its purposes. That was a sufficient trigger of scrutiny for constitutional reasonableness. The seizure facilitated a weeks-long, contemporaneous search for Jones's location. Considering the outsized effect on Jones, who was still presumed innocent, the seizure and the search were unreasonable without a warrant.

The present case is a much simpler seizure case. The government here seized data under authority given by 18 U.S.C. § 2703(d). J.A. 61-3. When government agents copy data or information that is otherwise unavailable to them, they have taken the rights to use and enjoy that data's benefits for the government, and the owner's right to exclude others has been eviscerated. *See* Mark Taticchi, *Note: Redefining Possessory Interests: Perfect Copies of Information as Fourth Amendment Seizures*, 78 Geo. Wash. L. Rev. 476, 491–96 (2010). From the beginning of its analysis, this Court should recognize data as something that can be seized.

Is it a "paper" or "effect"? Is it the defendant's paper or effect in which to assert a right? These questions come later in a methodical analysis.

B. *Kyllo* Is a High-Tech Search Case

Though less relevant here, this Court's opinion in *Kyllo v. United States*, 533 U.S. 27 (2001), is a wonder-

fully instructive modern "search" case, because it features a search in the absence of seizure. That allows us to observe search in the abstract and see how concealment subjected to search produces exposure. Bringing exposure to concealed things is a strong signal that a search has occurred.

The thermal-imaging camera used to incriminate the petitioner in *Kyllo* detected radiation in the infrared range of the electromagnetic spectrum (that is, radiation with longer wavelengths than visible light). It produced an image of that radiation called a thermogram by representing otherwise invisible radiation in the visible spectrum. That made imperceptible radiation perceptible to humans.

Using a thermal imager on a house was a search of its exterior for information about what transpired inside, and the Court found it so. "Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion," the Court held, "the surveillance is a 'search' and is presumptively unreasonable without a warrant." *Kyllo*, 533 U.S. at 40. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 553 (2005) ("For the holding in *Kyllo* to make sense, it must be the transformation of the existing signal into a form that communicates information to a person that constitutes the search. What made the conduct in *Kyllo* a search was not the existence of the radiation signal in the air, but the output of the thermal image machine and what it exposed to human observation.").

C. "Papers" and "Effects" Can Take a Digital Form

This Court has often been relatively clear that searched or seized items are within the categories listed for protection in the Fourth Amendment. In other cases, it is an essential inference of the Court's rulings. But the best practice would be to consistently and systematically recite each element of the Fourth Amendment as a model for lower courts.

The categorization of digital materials as paper, effects, or otherwise, as well as the ownership status of such items, are questions that would benefit from sharpening by this Court in this case. Significantly, the *Jones* Court declared the existence of a constitutionally protected item: "It is beyond dispute that a vehicle is an 'effect' as that term is used in the Amendment." 132 S. Ct. at 949. And it detailed the property question, finding that Jones "had at least the property rights of a bailee." *Id.* at 949 n.2. The possessive pronoun in the Fourth Amendment circumscribes the items in which defendants may assert Fourth Amendment interests.

Riley, of course, dealt with the unconstitutional search of a cell phone. By necessary inference, phones themselves are effects.

Dictum in *Riley* suggests that digital files in phones are effects, too. In declining to allow warrantless cellphone searches of a phone that may contain evidence of the crime of arrest, 134 S. Ct. at 2492, the *Riley* Court said 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). This Court treated not just phones, but the

documents and materials they hold, as effects. It did not matter that they were digital.

Seven years ago, the Sixth Circuit 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*, that court said: "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, 285–86 (6th Cir. 2010).

And last year the Tenth Circuit explicitly treated an email with attachments as "a 'paper' or 'effect' for Fourth Amendment purposes." None of the litigants had disputed that essential premise. *United States v. Ackerman*, 831 F. 3d 1292, 1304 (6th Cir. 2016).

The word "papers," of course, should not be taken narrowly as a "substance formed into thin sheets on which letters and figures are written or printed," but rather as "[a]ny written instrument, whether note, receipt, bill, invoice, bond, memorial, deed, and the like." N. Webster, *An American Dictionary of the English Language* (1828). The broad sense of the term is consistent with deep precedent. *Boyd v. United States*, 116 U.S. 616 (1886), for example, speaks numerous times of "books and papers" and "books, invoices, and papers." *Id.* at *passim*. Taking "papers" too narrowly would have Justice Bradley repeating himself incoherently: Books at the time were made largely of paper, invoices were made of paper, and papers were also, of course, made of paper. "Papers" was the broad cate-

gory of instruments on or in which people collect information to the *Boyd* Court, and to the Framers of the Fourth Amendment.

The parallel between email and tangible mail is the beginning but not the end of the relationship between digital files and the "papers" and "effects" categories. Again, the Fourth Amendment does not have special rules for communications, but covers all papers and effects equally. 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. This court would best treat digital files as papers or effects, regardless of its determinations about their ownership status and the reasonableness of seizing and searching particular files in any given case. The coverage of the Fourth Amendment must extend to these media if this Court is to succeed in "assuring preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo*, 533 U.S. at 34; *United States v. Jones*, 565 U.S. at 950; *id.* at 958 (Alito, J., concurring).

The final question before assessing the reasonableness of government action is whether a constitutionally protected item is the defendant's. Just as with telephones according to Justice Butler's view in *Olmstead*, people use modern communications and Internet facilities under contracts that allocate property rights. Though hardly with perfect clarity, these contracts detail how communications machinery will be used, and they divide up the ownership of information and data. *See* Scott R. Peppet, *Regulating the Internet*

of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, 93 Tex. L. Rev. 85, 142–45 (2014).

The court below, applying doctrine, back-handedly dismissed this crucial question: whether the defendants had a property right in the data that the government seized. J.A. 61-8 ("The defendants of course lack any property interest in cell-site records."). This Court should clarify the importance of property principles for administering the Fourth Amendment—it lists items of property, after all—reversing the court below and modeling for future courts how this is done with care.

IV. THE GOVERNMENT SEIZED AND SEARCHED PETITIONER'S DIGITAL PAPERS, WHICH WAS UNREASONABLE WITHOUT A WARRANT

Applying the terms of the Fourth Amendment to the instant case shows that the government seized and searched digital papers in which the petitioner had a relevant ownership interest. Given the requirement for a warrant in all but narrow, exceptional cases, doing so was unreasonable and thus violated their Fourth Amendment rights.

A. There Was a Seizure

The government's invocation of the authority of 18 U.S.C. § 2703(d) to command the disclosure of data was a seizure of that data. The Court should treat it as such because it deprived the owner of a salient property interest, the right to exclude.

This Court has emphasized the "right to exclude others" as "one of the most essential sticks in the bun-

dle of rights that are commonly characterized as property." *Kaiser Aetna v. United States*, 444 U.S. 164, 176 (1979); *see also Dolan v. City of Tigard*, 512 U.S. 374, 384 (1994); *Lucas v. South Carolina Coastal Council*, 505 U.S. 1003, 1044 (1992); *Nollan v. California Coastal Comm'n*, 483 U.S. 825, 831 (1987). Blackstone's definition of property also featured the right to exclude: "[property is] that sole and despotic dominion which one . . . claims and exercises over the external things of the world, in total exclusion of the right of any other individual in the universe." 2 William Blackstone, Commentaries *2.

There is an argument that data is not seized when its original owner still has a copy. But that argument is unavailing because it treats possession as the only important property right. It is not. The right to possess property is only one of several aspects of ownership identified in legal philosophy. *See generally* Tony Honoré, *Ownership*, in Oxford Essays on Jurisprudence 104-147 (A.G. Guest ed., 1961).

B. There Was a Search

Given the existence of a constitutional seizure of the data, a search of it need not be established to proceed to further steps in the Fourth Amendment analysis. But searches of data will be a relevant issue before this Court and others in the future, so it is at least an important detail.

By causing computers to render it in human-readable form, government agents searched the data they had seized in order to learn the whereabouts of Carpenter and Sanders during the relevant time-periods.

Putting aside confusing doctrine in favor of natural language, "'Search' consists of looking for or seeking

out that which is otherwise concealed from view." *Black's Law Dictionary* 1349 (6th ed. 1990). In *Kyllo*, this Court said, "When the Fourth Amendment was adopted, as now, to 'search' meant '[t]o look over or through for the purpose of finding something; to explore; to examine by inspection; as, to *search* the house for a book; to *search* the wood for a thief.'" *Kyllo*, 533 U.S. at 32 n.1, quoting N. Webster, *An American Dictionary of the English Language* 66 (1828) (reprint 6th ed. 1989).

Communications and data, just like other things, can be looked through with the purpose of finding something. They are searched when their contents are converted in format, bringing information out of concealment into exposure.

In his article, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531 (2005), Professor Orin Kerr intricately analyzes the technical details of computer processing as it relates to government investigations. *Id*. at 549-51. "The best answer," he concludes, "is that a search occurs when information from or about the data is exposed to possible human observation." *Id*. at 551. Here, the government's agents did that with the data they had earlier seized.

C. "Papers" or "Effects" Were Involved

Putting aside for the moment whose it was, there is little basis for arguing that the data seized are not constitutional papers or effects. As discussed above, the relevant meaning of "papers" in the Fourth Amendment is not thin sheets of ink-absorbent material but any corpus or collection of information.

The court below referred to the data in question as "business records" several times. This would tend to

confirm that they are collections of information qualifying as constitutional papers. That usage elided the distinct question of whose records they are, however.

D. Carpenter and Sanders Owned Them

The Fourth Amendment uses the possessive pronoun "their" to modify "persons, houses, papers, and effects." Doing so limits who can claim the protections of that law with respect to any such item. In relevant part, the data that the government seized was the property of Messrs. Carpenter and Sanders. It was not the property of their cellular providers, MetroPCS and T-Mobile, to give to the government.

In this area, again, careful attendance to property concepts helps draw the lines. They may be "business records"—information collected by a business for business purposes—but that does not make them automatically the property *in toto* of the business.

Consumer-facing digital businesses, including telecommunications providers, enter into very detailed arrangements that divide up ownership of information about customer use of their services. Communications providers are also subject to regulations that similarly allocate rights to exclude, use, sell, and process information.

When people use digital and communications services, they share and produce personal information that can be sensitive, intimate, and privileged. This is why the T-Mobile and MetroPCS user agreements and privacy policies allocate the bulk of rights to control and use personal data to customers, consistent with practice across digital services. These property rights in data include the right of users to exclude others

from personal data in all but closely defined circumstances.

The T-Mobile privacy policy in effect in late 2010,[3] which was incorporated by reference into the company's terms of service, *see* T-Mobile Terms & Conditions, December 7, 2010 snapshot, http://bit.ly/2wJi6ev, is typical in that it denies T-Mobile rights to sell or share data except as provided in the policy. "We do not sell, rent, or otherwise provide your personal information to unaffiliated third-parties (parties outside the T-Mobile corporate family) to market their services or products to you. We may, however, disclose your personal information to unaffiliated third-parties as follows:" T-Mobile Privacy Policy, December 4, 2010 snapshot, http://bit.ly/2vQ64DQ [hereinafter "2010 T-Mobile Contract"]. This leaves the general right to exclude all others from the data with the customer. The possessive pronoun "your" signifies that the bulk of the ownership of the data is the customer's.

Contract terms limiting access to personal information have a long history. *See, e.g., Peterson v. Idaho First Nat'l Bank*, 367 P.2d 284, 290 (Idaho 1961), *quoting* 7 Am.Jur., Banks, § 196 ("[I]t is an implied term of the contract between a banker and his customer that the banker will not divulge to third persons, without the consent of the customer, express or implied, either

[3] The current MetroPCS Terms and Conditions and privacy policy are similar in all material ways to T-Mobile's commitments, though the precise language varies. *See* https://www.metropcs.com/terms-conditions/terms-conditions-service.html and https://www.metropcs.com/terms-conditions/privacy.html. Probably due to a change in the URL structure of the MetroPCS site, versions of these documents contemporaneous to the events in this case could not be found.

the state of the customer's account or any of his transactions with the bank, or any information relating to the customer acquired through the keeping of his account, unless the banker is compelled to do so by order of a court, [or] the circumstances give rise to a public duty of disclosure").

In the modern era, much enforcement of these rights is by government agencies standing in for consumers. *See, e.g.*, Federal Trade Comm'n, "Enforcing Privacy Promises" webpage, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises. But there is also active litigation that asserts violation of contracts pertaining to terms of service, privacy policies, and the like. *See, e.g., In re Facebook Internet Tracking Litigation*, No. 5:12-md-02314-EJD (N.D. Cal. filed Feb. 8, 2012). These rights are property rights. *See U.S. Trust Co. v. New Jersey*, 431 U.S. 1, 19 n.16 (1977) ("Contract rights are a form of property"). There is no juridical way to characterize the exchange of promises between T-Mobile and its customers other than as contracts allocating property rights.

The exceptions to the general rule, allocating certain rights to T-Mobile, are also typical of privacy policies. T-Mobile may share personal information with service providers and merger partners subject to relevant constraints. The contract allows T-Mobile to share information with other third parties "with your consent," 2010 T-Mobile Contract. By inference, the right to sell, like the bulk of the rights to the data, rests with the customer.

One of the exceptions—also typical and appropriate—is the exception for sharing with government and law enforcement. That provision states in relevant

part: "We may disclose personal information or communications where we believe in good faith such disclosure is necessary to comply with the law or respond to legal process (for example, lawful subpoena, court order, E-9-1-1 information)." 2010 T-Mobile Contract.

This provision does not give T-Mobile free rein to hand data over to the government when asked. T-Mobile can only do so when its good faith assessment is that it must comply with law or respond to legal process. T-Mobile may not hand over information when the law does not require it, or when it is faced with something other than "legal process."

At least two senses of that word "legal" are relevant. One is that the procedures are recognized and systematically used procedures in law enforcement and courts. The other is that the procedures comport with the standards laid out in the law.

The contract does not permit T-Mobile to comply with court orders simply because they take a certain form. Such orders must also satisfy the substantive legal merits for divesting a private party of control over the things demanded by the government. T-Mobile only has the right to share the data if the process used to divest the customer of control is both legal in form and substance. To the extent T-Mobile does not resist an invalid or overbroad subpoena, the data is not T-Mobile's to turn over. The data remains the property of the customer.

There is an argument that the T-Mobile privacy policy denies customers the right to exclude others from data that is disclosed pursuant to § 2703(d) because it is a legal process, established by Congress no less. But that begs the question whether the process is

valid and legal. The customer should be able to argue his or her side of that question. Presuming the opposite would make surplus language of important words in the sentence giving T-Mobile only a limited right to provide information to the government.

A customer who is suspected of criminal activity cannot sensibly be invited to participate in adjudicating his or her rights during the investigation, of course. The next step in the analysis makes clear that the solution is to enlist a neutral arbiter.

E. The Government's Actions Were Unreasonable

The final step in the analysis is determining whether it was unreasonable for government agents to seize and search data which in relevant part was Carpenter's and Sanders's to exclude from all others. It was indeed unreasonable.

The structure of the Fourth Amendment suggests, and the Supreme Court's precedents make clear, that getting a warrant is the reasonable thing to do when it can be done. "It is a cardinal rule that . . . law enforcement . . . use search warrants wherever reasonably practicable." *Chimel v. California*, 395 U.S. 752 (1969).

Cell-site location information sits in long-term storage with stable, identified service providers. There is no exigency that threatens its destruction. Imposing the warrant requirement does put a small paperwork burden on law enforcement, but it does so to provide all telecommunications users the benefit of having a check on governmental processes that might otherwise upset the contract-based property rights that undergird their digital privacy protection.

* * *

The analytical framework suggested and used above shows that the government seized and then searched data—constitutional papers—in which Timothy Ivory Carpenter and Timothy Michael Sanders had a relevant property interest. Doing so without a warrant was unreasonable, and thus it violated their constitutional rights. That conclusion hardly forecloses the use of cell site location information in criminal investigations. It merely imposes the procedural check against abuse of having a neutral arbiter sign off on a warrant.

There are cases where cell site location information might be very useful even though neither exigency nor probable cause exist, such as when the data could reveal where a homicide victim was located immediately prior to death. But such situations can be and are accounted for in the contracts that allocate rights to customer data. The T-Mobile contract, for example, allows disclosure in emergency situations and to the primary account holder. For the narrow cases that remain, the terms of such policies could make clear that rights to exclude others from data expire with the customer or are the property of his or her next of kin.

If this Court declines to abandon the sociological approach to Fourth Amendment administration found in the "reasonable expectation of privacy" test, an alternative to merely guessing at what people expect is to consult the very documents that record and define their expectations: the contracts between communications providers and their customers.

People expect privacy in data about their communications because they have contract-based and other property rights to exclude others from it. Reasoning through the elements of the Fourth Amendment in

light of those arrangements is a better model of jurisprudence than guesswork about privacy expectations.

CONCLUSION

Applying the text of the Fourth Amendment to this case, the Court should reverse the decision below.

Respectfully submitted,

Ilya Shapiro
CATO INSTITUTE
1000 Mass. Ave. N.W.
Washington, D.C. 20001
(202) 842-0200
ishapiro@cato.org

Manuel S. Klausner
LAW OFFICES OF MANUEL S. KLAUSNER
One Bunker Hill Building
601 W. Fifth St., Suite 800
Los Angeles, CA 90071
(213) 617-0414
mklausner@klausnerlaw.us

Jim Harper
Counsel of Record
Ryan C. Radia
COMPETITIVE ENTERPRISE INSTITUTE
1310 L St. NW, 7th Floor
Washington, D.C. 20005
(202) 331-1010
jim.harper@cei.org

Curt Levey
The Committee for Justice
722 12th St. NW, 4th Floor
Washington, DC 20005
(202) 270-7748
clevey@committeeforjustice.org

August 11, 2017