No. 16-6308

IN THE

Supreme Court of the United States

AARON GRAHAM, *Petitioner*,
v.
UNITED STATES OF AMERICA, *Respondent*.

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

Brief *Amicus Curiae* of U.S. Justice Foundation, Gun Owners Foundation, Gun Owners of America, Inc., Downsize DC Foundation, DownsizeDC.org, Conservative Legal Defense and Education Fund, The Heller Foundation, and Policy Analysis Center in Support of Petitioner

MICHAEL CONNELLY
U.S. JUSTICE FOUNDATION
932 D Street, Ste. 2
Ramona, CA 92065
Attorney for Amicus Curiae U.S. Justice Foundation

HERBERT W. TITUS*
ROBERT J. OLSON
WILLIAM J. OLSON
JOHN S. MILES
JEREMIAH L. MORGAN
WILLIAM J. OLSON, P.C.
370 Maple Ave. W., Ste. 4
Vienna, VA 22180-5615
(703) 356-5070
wjo@mindspring.com

**Counsel of Record*
Attorneys for Amici Curiae

November 3, 2016

TABLE OF CONTENTS

TABLE OF AUTHORITIES

INTEREST OF *AMICI CURIAE*[1]

U.S. Justice Foundation, Gun Owners Foundation, Downsize DC Foundation, Conservative Legal Defense and Education Fund, The Heller Foundation, and Policy Analysis Center are nonprofit educational organizations, exempt from federal income tax under section 501(c)(3) of the Internal Revenue Code ("IRC"). Gun Owners of America, Inc. and DownsizeDC.org are nonprofit social welfare organizations exempt from federal income tax under IRC section 501(c)(4).

These organizations were established, *inter alia*, for educational purposes related to participation in the public policy process, including programs to conduct research and to inform and educate the public on important issues of national concern, the proper construction of state and federal constitutions and statutes, questions related to human and civil rights secured by law, and related issues. Each organization has filed numerous *amicus curiae* briefs in this Court and other federal courts.

---

[1] It is hereby certified that counsel for the parties have consented to the filing of this brief; that counsel of record for all parties received notice of the intention to file this brief at least 10 days prior to its filing; that no counsel for a party authored this brief in whole or in part; and that no person other than these *amici curiae*, their members, or their counsel made a monetary contribution to its preparation or submission.

STATEMENT

In this case, the federal government suspected Graham of committing certain crimes, yet lacked probable cause to obtain a warrant. Nevertheless, a federal law authorized government officials on reasonable suspicion to obtain a "corporate records subpoena" (not a warrant) from a "magistrate judge" (not an Article III judge). This administrative authorization, issued by one who is essentially an administrative official, permitted the government to obtain a vast amount of highly personal information about Graham (29,659 location points over 221 days), "or approximately one location point every 11 minutes for seven months." Pet. at 4. That alone is startling, but it is just the tip of the iceberg.

This Court should grant certiorari to review this case because, if this abuse of power is not checked, the Fourth Amendment will be rendered obsolete by technological advances. First, there will be an increasing number of digital devices which utilize cellular service to operate, including not only cell phones, but also tablets, laptops, automobiles, "smart" watches, and even pacemakers.[2] Second, as cellular technology improves and becomes cheaper, there will be an exponential increase in the number of cell towers, serving smaller and smaller areas, which could provide an even more accurate picture of a device's

---

[2] *See* R. Adler, "Meeting the demand for mobile everything," Computer World, Sept. 25, 2015, http://www.computerworld.com/article/2986723/internet-of-things/meeting-the-demand-for-mobile-everything.html.

location.[3] Third, as smart phone technology continues to improve, an increasing number of a phone's operating functions trigger the creation of location "data points" as one goes about his daily life.[4] Fourth, as digital storage technology improves, increasing the ease and capacity of storage will increase the amount of information exponentially,[5] so that an entire lifetime of "location points" can be stored indefinitely for every American who uses the modern technology.

Petitioner notes that such Orwellian power "threatens to fundamentally alter the relationship

---

[3] *See* In re Tel. Info. Needed for a Crim. Investigation, 119 F. Supp. 3d 1011, 1015 (N.D. Cal. 2015) ("smaller and smaller base stations are becoming increasingly common. Examples include microcells, picocells, and femtocells, all of which cover a very specific area, such as one floor of a building, the waiting room of an office, or a single home."); M. Rajagopalan, "Cellphone Companies Will Share Your Location Data - Just Not With You," Pro Publica, June 27, 2012, https://www.propublica.org/article/cellphone-companies-will-share-your-location-data-just-not-with-you ("as the number of mobile phones continues to rise, cell phone companies are now installing thousands of small boxes known as microcells in crowded places like parking garages and shopping malls to enable them to provide better service. Microcells ...also enable the phone companies to record highly precise location data.").

[4] L. Cassavoy, "21 Awesome GPS and Location-Aware Apps for Android," PC World, Jul. 31, 2012, http://www.pcworld.com/article/260112/21_awesome_gps_and_location_aware_apps_for_android.html.

[5] L. Mearian, "Data Storage – Then and Now," Computer World, Mar. 14, 2014, http://www.computerworld.com/article/2473980/data-storage-solutions/data-storage-solutions-143723-storage-now-and-then.html.

between the government and the governed." Pet. at 10. Even the district court below realized that the continuous technological revolution "raise[s] the specter of prolonged and constant government surveillance...." United States v. Graham, 846 F. Supp. 2d 384, 389 (D. Md. 2012). The idea that the Framers of the Fourth Amendment would have tolerated a government monitoring and recording where every American is, and has been at all times, and often even prying into what they are doing, is unthinkable. But that is precisely the perverse result which the Fourth Circuit below invites. By stacking this Court's "third-party records" precedents on the "reasonable expectation of privacy" doctrine, "an individual enjoys no Fourth Amendment protection" against such tyrannical surveillance. United States v. Graham, 824 F. 3d. 421, 425 (4th Cir. 2016) (en banc).

SUMMARY OF ARGUMENT

The "corporate records subpoena" issued in this case to obtain 29,659 location points as to Graham's whereabouts over a 221 day period violates the Fourth Amendment. Unless an American foreswears all connection to modern technology, his devices are constantly emitting information, including the Cell Site Location Information ("CSLI") data seized here. Such information can be used to determine the precise whereabouts of every American, from the time that he gets his first cell phone through death. If the government may obtain access to such personal information using an administrative subpoena issued by a magistrate, the Fourth Amendment will be rendered a dead letter.

The rationale by which such a search and seizure of an American's data has been sustained by the Fourth Circuit is based not in the U.S. Constitution, but in doctrines relatively recently developed by this Court, including the "third party doctrine" set out in cases such as the 1979 decision in Smith v. Maryland. As Justice Sotomayor explained in U.S. v. Jones, this doctrine can and should be reconsidered by this Court.

Fortunately, this Court's 2012 decision in United States v. Jones, the 2013 decision in Florida v. Jardines, and the 2015 decision in Grady v. North Carolina, have reconsidered the "reasonable expectation of privacy test," and have found it wanting. These decisions have reinvigorated the centrality of property rights in understanding the protections afforded by the Fourth Amendment. When property-based principles are applied to the CSLI data seized and searched in this case, the flaws in the third-party doctrine are revealed, and the need for this Court to grant certiorari and to decide this important issue becomes clear. These is the sort of "important question of federal law that has not been, but should be, settled by this Court" as described in Supreme Court Rule 10.

ARGUMENT

I. The Petition Should Be Granted Because The "Third-Party Doctrine" Was Wrong In Its Inception, Is Wrong Today, and Should Finally Be Discarded.

As discussed *infra*, the "third-party doctrine" is among some of this Court's most criticized precedents. An offspring of the Katz[6] experiment with the "reasonable expectations of privacy" test, the third-party doctrine is based on the proposition "that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Smith v. Maryland, 442 U.S. 735, 743-44 (1979). Because of that supposed lack of reasonable expectation, the Fourth Amendment does not even come into play as a limit on government power.

In United States v. Miller, 425 U.S. 435 (1976), this Court claimed that, with respect to a person's bank records, "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the government." *Id.* at 443. The Court reached this conclusion "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.*

Three years later, Smith v. Maryland, 442 U.S. 735 (1979), applied the third-party doctrine to a phone company's records of telephone numbers dialed from a

---

[6] Katz v. United States, 389 U.S. 347 (1967).

home phone. Over the years, the doctrine has been applied to a host of other types of records, including medical records[7] and, of course, the cell site location information in this case. The doctrine has grown incrementally, to the point that "under an aggressive reading of the third-party doctrine, the Fourth Amendment would not guarantee the privacy of any personal data held by any private company [including] virtually all records of electronic communications, web browsing activity, and cloud data, to name just a few examples." M. Price, "Rethinking Privacy: Fourth Amendment 'Papers' and the Third-Party Doctrine," 8 J. NAT'L SECURITY L. AND POL'Y 247, 265 (2016) .[8]

Indeed, every "one and zero" transmitted over the Internet in some sense has been "voluntarily conveyed" to a third party for the limited purpose of transmission to another. Under the third-party doctrine, it could be argued that even Katz should have come out differently, since the conversation in that case occurred over cables belonging to the third-party phone company. The only arbitrary line that could be (and has been) drawn by judges is that some parts of

---

[7] K. Butler, "DEA: Medical Records Sent to Pharmacies Have No Protected Privacy," UPI, (Sept. 24, 2013), http://www.upi.com/blog/2013/09/24/DEA-Medical-records-sent-to-pharmacies-have -no-protected-privacy/7221380050479/.

[8] Michael Price is counsel at the Brennan Center for Justice. It is quite a twist of fate that the group responsible for "rethinking privacy" is named after the Justice perhaps most responsible for today's privacy regime. *See* Warden v. Hayden, 387 U.S. 294 (1967). *See also* H. Titus and W. Olson, United States v. Jones: Reviving the Property Foundation of the Fourth Amendment, 3 Case W. Res. J.L. Tech. & Internet 243, 257-261 (2012).

communications are too private (such as the content of emails),[9] whereas others (such as email to/from lines) are not private enough to merit Fourth Amendment protection.[10] To paraphrase Orwell's Animal Farm, "a person's papers are all equal, but some of his papers are more equal than others."

Of course, such subjective line drawing creates a distinction without a principled difference. Even data as basic as the number a person dials reveals if the call is to a phone sex service, a drug rehabilitation center, or an oncologist's office. That information can be just as personal and revealing as an actual recording of the conversation itself. The truth is that the third-party doctrine has placed at the government's fingertips a vast treasure trove of highly personal information about virtually every American which is captured and stored by countless third parties spread across the globe. At least one communications giant, AT&T, has jumped headfirst into this marketplace of Fourth Amendment evasions, compiling vast amounts of personal information in order to "develop[], market[], and s[ell]" that information to federal, state, and local governments. K. Lipp, "AT&T Is Spying on Americans for Profit, New Documents Reveal," The Daily Beast, October 25, 2016.[11] Indeed, "[w]hile telecommunications companies are legally obligated to hand over records, AT&T appears to have gone much

---

[9] *See, e.g.*, U.S. v. Warshak, 631 F.3d 266, 274 (6th Cir. 2010).

[10] *See, e.g.,* U.S. v. Forrester, 512 F.3d 500 (9th Cir. 2008)

[11] *See* http://www.thedailybeast.com/articles/2016/10/25/at-t-is-spying-on-americans- for-profit.html.

further to make the enterprise profitable...." *Id.* In other words — this technological giant has become your government's "one-stop shop" for Fourth Amendment circumventions.

With nearly every technological development creating yet another opportunity for government intrusions, many have questioned "whether [the third-party] doctrine is still viable in light of the major technological and social changes over the past several decades."[12] Significantly, Justice Sotomayor, writing in concurrence in United States v. Jones, 132 S.Ct. 945 (2012), noted that the doctrine is "ill suited to the digital age" and that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." *Id.* at 957.

In truth, however, it is not these technological changes themselves which have made the third-party doctrine obsolete. Rather, such changes have only highlighted and magnified the underlying problem with the doctrine. The third-party doctrine was wrong in 1976, and it is wrong today. The only difference is

---

[12] *See* R. M. Thompson II, "The Fourth Amendment Third-Party Doctrine," Congressional Research Service, R43586, June 5, 2014, https://www.fas.org/sgp/crs/misc/R43586.pdf. *See also* O. Kerr & G. Nojeim, "The Data Question: Should the Third-Party Records Doctrine Be Revisited?" ABA Journal (Aug. 1, 2012) ("As more and more information moves online, some have questioned whether this principle should continue to be applied."); ("Existing Fourth Amendment tests are not fit for the digital long haul") http://www.abajournal.com/mobile/mag_article/the_data_question_should_the_third-party_records_doctrine_be_revisited/.

that today the doctrine has the potential to do much greater damage, because new and changing technologies keep making it easier and easier for the government to persuade judges to override the vague "privacy" interests of individuals.

Some courts have done a good job in distinguishing Smith and its progeny from the facts of this case. *See, e.g.*, In Re: Telephone Information at 1029 ("historical CSLI generated via continuously operating apps or automatic pinging does not amount to a *voluntary* conveyance of the user's location twenty-four hours a day for sixty days.") But for the reasons laid out above, the third-party doctrine should not just be refined — it should be dismantled. This case presents just the opportunity that Justice Sotomayor anticipated in her concurrence in Jones. The Court should grant the Petition to decide not only whether the third-party doctrine is "ill suited to the digital age" — but also whether it is ill suited to any age.

II. The Third-Party Doctrine Conflicts with the Fourth Amendment Property Principle Underlying the Decisions in Jones and Jardines.

The Court should continue its revitalization of the Fourth Amendment's property roots that it began in Jones and Jardines.[13] Under a property analysis, a very different result obtains in this case.

---

[13] Florida v. Jardines, 133 S.Ct. 1409, 1414 (2013).

A. The Fourth Amendment Foremost Protects the People's Property Rights in Their Persons, Houses, Papers, and Effects.

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures." Before the modern era of laser beams, electronic eavesdropping, and cell phones, this right was understood to protect the people's common law rights in tangible, physical property. *See* United States v. Jones, 565 U.S. 400, 132 S.Ct. 945, 949-50 (2012). Then, in 1967, the Supreme Court, purporting to extend greater protection to the Fourth Amendment rights of the people over intangible communications, deciding that the Amendment primarily concerned the "privacy interests" of the people. Benching "property rights" to the role of a pinch hitter, the Court fashioned its own rule that a Fourth Amendment search could be established only if the search invaded a "reasonable expectation of privacy" in their "persons, houses, papers, and effects." 132 S.Ct. at 950-51.

In 2012, the Supreme Court recharted its path. Reasserting that the original text of the Amendment was plainly designed foremost to protect private property, the Court consigned the reasonable-expectation-of-privacy test to a secondary role, no longer the *sine qua non* to whether there was a Fourth Amendment search. *Id.* at 951-52. At best, the Court ruled in Jones, the privacy test functioned only as an add-on, but not a substitute for, the common law property rights of the people in their persons, houses,

papers, and effects. *See also* Jardines at 1414.

B. The Property Principle Applies to the Government Intrusion in this Case.

In Jones, law enforcement officials without a warrant installed a GPS device on a suspect's car in order to track his movements upon the public highways. The government contended that the GPS attachment was not a Fourth Amendment search because the suspect had no reasonable expectation of privacy in his movements upon the public highways. The Court rejected this argument on the ground that foremost the Fourth Amendment protects specific private property rights, not generalized privacy interests. Thus, the Court held that a Fourth Amendment search took place at the point of the installation of the GPS tracking device, a trespassory intrusion upon the private property rights of the automobile's owner, the government having "physically occupied private property for the purpose of obtaining information." Jones, 132 S.Ct. at 949.

In this case — without either a warrant or probable cause, but only upon a magistrate order based upon reasonable suspicion — government officials sought information about the movement of two criminal suspects generated by their use of their cell phones. The government claimed that there was no Fourth Amendment search because the suspects had no reasonable expectation of privacy in the information generated by their phone use and stored by the providers of their cell phone services. The *en banc* court of appeals agreed, concluding that, because

under this Court's third-party doctrine, "an individual can claim 'no legitimate expectation of privacy' in information that he has voluntarily turned over to a third party." "[T]he government," the *en banc* court continued, "does **not** engage in a Fourth Amendment '**search**' when it acquires such information from a third party." Graham at 427 (emphasis added).

In so ruling, the *en banc* court committed the same error as the court of appeals did in Jones — having assumed that "'a Fourth Amendment **search** occurs [only] when the government violates a subjective expectation of privacy that society recognizes as reasonable.'" *See* Graham at 425. To be sure, the *en banc* majority cited Jones, but only to rebut petitioner's claim that "the government always invades an individual's reasonable expectation of privacy when it employs technological devices to track an individual's moves." *See id.* at 426.

In its October 2014 term, this Court granted a petition for a writ of certiorari to review a decision by the Supreme Court of North Carolina that the Fourth Amendment does not prohibit the state from subjecting a recidivist sex offender to the state's satellite-based monitoring system, forcing him to "wear tracking devices at all times ... for the rest of his life." Grady v. North Carolina, 575 U.S. ___, 135.Ct. 1368, 1369 (2015). The state court rejected the offender's Jones-based argument — that, "'if affixing a GPS to an individual's vehicle constitutes a **search** of the individual, then the arguably more intrusive act of affixing an ankle bracelet to an individual must constitute a **search** of the individual as well.'" *Id.* at

1370. (emphasis added). Instead, the state court distinguished Jones, contending that the question of whether there is a Fourth Amendment search depends upon the "propriety" of the search, not just upon whether the fixing of the ankle bracelet physically intruded on the recidivist's person. Having freed itself from Jones, the state court ruled that "the State's system of nonconsensual satellite-based monitoring does **not** entail a **search** within the meaning of the Fourth Amendment," and thus, does not apply. *Id.* at 1370 (emphasis added).

The Supreme Court responded: "That theory is inconsistent with this Court's precedents:"

> In *United States v. Jones*, we held that "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a '**search**.'" (citation omitted). We stressed the importance of the fact that the Government had "physically occupied private property for the purpose of obtaining information." [*Id.* at 1370 (emphasis added).]

The Court continued:

> Under such circumstances, it was **not necessary to inquire about** the target's **expectation of privacy** in his vehicle's movements in order to determine if a Fourth Amendment **search** had occurred. "Where, as here, the Government obtains information by physically intruding on a constitutionally

> protected area, such a **search** has undoubtedly occurred." [*Id.* (emphasis added).]

In Grady, the Court further noted that it had "reaffirmed this principle in *Florida v. Jardines* (citation omitted) where [it] held that having a drug-sniffing dog nose around a suspect's front porch was a **search**, because police had 'gathered ... information by physically entering and occupying the [curtilage of the house] to engage in conduct not explicitly or implicitly permitted by the homeowner,'" reiterating the property principle in Jones that "a **search** occurs 'when the government gains evidence by physically intruding on constitutionally protected areas.'" Grady at 1370 (emphasis added).

In the case of Mr. Graham, whether a Fourth Amendment **search** has occurred depends first upon whether or not there was a physical intrusion. Undoubtedly there was. As the *en banc* court acknowledged:

> [T]he nature of the state activity that is challenged ... is the Government's acquisition from a phone company, Sprint/Nextel, of historical CSLI records – i.e., the records of the phone company that identify which cell towers it used to route Defendant's calls and messages. [Graham at 425.]

Indeed, Graham's CSLI was not discovered aimlessly floating around in cyberspace. Rather, the historical records that the government sought were stored on a Sprint hard drive, a very tangible object. No doubt

such hard drives constitute both "papers and effects."

Additionally, the government's intrusion took place in a "constitutionally protected area," namely, "as the Sprint/Nextel custodian of the CSLI records testified at trial, CSLI is created and maintained in the normal course of Sprint/Nextel's business." *Id.* Yet, the *en banc* majority failed to make any finding that there was or was not a physical intrusion into a constitutionally protected area before deciding whether a Fourth Amendment search had not taken place. Instead, it concluded that such a search had not taken place because the defendants "do not have a reasonable expectation of privacy in historical CSLI records that the government obtains from cell phone service providers through a § 2703(d) order." Graham at 428. That theory is foreclosed by both Jones and Jardines.

C. Graham Has a Protected Property Interest in the CSLI Produced By His Cell Phone.

The government no doubt would argue that the Jones/Jardines property principle does not apply here because the government physically intruded upon the property of the third-party telephone service provider, not the defendants. This claim overlooks several relevant factors that, when examined, demonstrate affirmatively that, while the CSLI of every cell phone user is in the possession of their service providers, it does not mean that the cell phone user has no property interest in the CSLI.

First, it is not the cell phone service provider, but

the cell phone user who, by his own movements and communications, produces the CSLI. As a "person" within the meaning of the Fourth Amendment, the cell phone user by the "labor of his body and the work of his hands" is entitled as a matter of property right to the information generated by his movements and communications. *See* J. Locke, Second Treatise of Government Para. 27 (facsimile ed.), reprinted in J. Locke, Two Treatises of Government, pp. 287-88 (P. Laslett, ed., Cambridge Univ. Press:2002). According to Jones, the word "persons" as it appears in the Fourth Amendment is, like "houses," "papers," and "effects," a term of property, not of privacy. Jones, 132 S. Ct. at 949. At the time the Fourth Amendment was ratified as part of the Constitution, it was well understood that a man's property "encompassed not only the objects a person owned but also the ability, indeed the right to acquire them." *See* J. Rakove, Revolutionaries. A New History of the Invention of America 78 (New York: 2010). Applying these principles here, a cell phone user owns the CSLI generated by his cell phone use. As its initial owner, the cell phone user transfers possession, but not ownership, of the CSLI to the service provider, creating an entrustment analogous to a bailment for hire.

Second, as the one who generates the CSLI attributed to his phone use, the CSLI is a valuable resource to the cell phone user should the need arise to document the user's movements. For example, a cell phone user may be accused of a crime that allegedly took place at a specific time and place. The CSLI generated by his phone use may prove an invaluable

asset to confirm an alibi that he was not at the particular place at that particular time. Recognition of the user's property interest is consistent with the terms and conditions of service in Sprint's standard service agreement. Sprint acknowledges that it provides "Location-Enabled Services," because its "networks generally know the location of your Device when it is outdoors and/or turned on."[14] Within certain limits, Sprint promises that "[b]y using various technologies to locate your Device, we can provide enhanced emergency 911 services and optional location-enabled services provided by us, [including] access [to] your Device's location information." *Id.* In other words, CSLI is not gathered simply to provide the government with evidence in criminal trials, or for use by the provider.

Third, the standard Sprint cell phone service agreement limits third-party access to any information generated by cell phone use. While the cell phone user "agree[s] that any authorized user may access ... location-enabled applications through the Services," such "location-enabled application is subject to the terms and conditions and policies, including its privacy policy." *Id.* Sprint's privacy policy in turn includes the promise not to share information, "including location information" with any third party, with specified exceptions.[15]

---

[14] https://shop2.sprint.com/en/legal/os_general_terms_conditions_popup.shtml

[15] *See* https://www.sprint.com/legal/privacy.html.

In sum, Sprint policy is to "release [CSLI] to a customer when we receive a valid legal demand for it."[16] While Sprint also may claim a proprietary interest in the CSLI generated by a cell phone user, its policy to release such information if there is a legal demand for it would reflect a bailment for hire. Surely, then, the CSLI generated by the cell phone user and stored by the cell phone provider is a "paper" or "effect," in which the cellphone user has a protectable property interest under the Fourth Amendment. And any effort of the government to tap into the phone user's CSLI is a physical intrusion on a constitutionally protected space belonging to the user who originated the location information.

D. As in Jardines, Without a Warrant the Government May Do "No More than Any Private Citizen Might Do."

In Florida v. Jardines, this Court held that the police may not use a drug sniffing police dog to snoop around a person's home. On the contrary, this Court held, "a police officer not armed with a warrant may [only] approach a home and knock, precisely because that is **'no more than any private citizen might do**.'" 133 S.Ct. 1409, 1416 (2013) (emphasis added).

Applied to Smith v. Maryland, if it were not the government seeking Smith's bank records, but instead

---

[16] M. Rajagopalan, "Cellphone Companies Will Share Your Location Data - Just Not With You," Pro Publica, June 27, 2012, https://www.propublica.org/article/cellphone-companies-will-share-your-location-data-just-not-with-you.

Smith's neighbor, it is a virtual certainty that the bank would never divulge the information. If the bank did provide Smith's records to his neighbor, there likely would be any number of remedies available to Smith. First, there likely would have been a breach of contract.[17] If Smith's reputation suffers, there could be a suit for defamation. There definitely would be a cause of action for "invasion of privacy," however that relatively new tort is defined. Likewise, in this case, if Graham had, for example, an ex-girlfriend who asked Sprint to provide her with Graham's CSLI, there is no doubt that Sprint would refuse.

The notion that a bank must turn over a person's financial records to the government without a warrant to search for evidence of money laundering is akin to saying that a valet must hand over the keys to a diner's vehicle so that the police can search the trunk for drugs. After all, "the [diner] takes the risk, in revealing his [car] to another, that the [car] will be conveyed by that person to the Government... even if the [key] is [turned over] on the assumption that it will only be [used to park the car]...." *See* Miller at 443.

---

[17] For example, the Bank Services Agreement for BB&T Bank informs customers that, while their information generally is kept confidential, there are certain limited situations where the bank may share it for purposes of effecting the depositor's business. https://www.bbt.com/assets/docs/pdf/bbt-com/customer-service/personal-services-pricing-guide/bank_services_agreement.pdf, (p. 29). Likewise, the bank's Privacy Notice lists " the reasons financial companies can share their customers' personal information." https://www.bbt.com/privacy-and-security/privacy/consumer-privacy-notice.page. Conspicuously absent from the list is any sharing with "the general public."

On the contrary, a valet — as a bailee of a vehicle — has no more right to turn it over to the police for a search than he does to take it on a joy ride.

In the past, the Court has tried to distinguish bank records and other third-party held records on the grounds that they are not actually the "papers" of the defendant, but rather are records created and maintained by the third party in the course of doing business. *See* Miller at 440. *Amici* dispute the truth of that distinction, but even so, that does not mean a person has no rights in records such as financial records that banks keep about his transactions.

It is obvious from Smith and Miller that "any private citizen" could never rightfully obtain the information that the government obtained. In each case, the "third party" has a legal relationship with its customer, and part of that relationship requires the customer's data to be protected, whether that be expressly provided in a contract, or "license ... implied from the habits of the country...." Jardines at 1415. In each case, a customer's personal information is conveyed to a third party with the understanding that it will be used for the limited purpose of providing service to the customer — and not shared publicly for the world to see. *See* Miller at 443.

Whereas the Smith privacy lesson is that a person has reduced expectations of privacy in information he shares with third parties, Jones protects a person's property regardless of where it is located. While Jones retained his property rights even though he had parked his car in a public lot, so too does Graham

retain his property rights in his CSLI even though they are retained on a Sprint server.

The third-party doctrine, however, pretends that there is no violation when the government interferes with a person's property, even without a warrant or probable cause. Not so. Like in Jardines, absent a warrant, the government should have no greater access to a person's bank records, phone call history, or his CSLI, than has "any private citizen."

CONCLUSION

Relying on Justice Sotomayor's concurrence in Jones, the *en banc* majority below suggested that:

> [A]lthough the Court formulated the third-party doctrine as an articulation of the reasonable-expectation-of-privacy inquiry, it increasingly feels like an exception. A per se rule that it is unreasonable to expect privacy in information voluntarily disclosed to third parties seems unmoored from current understandings of privacy. But Justice Sotomayor ... made clear that tailoring the Fourth Amendment to "the digital age" would require the Supreme Court itself to "reconsider" the third-party doctrine. [Graham at 437.]

Justice Sotomayor is right. It is time for this Court to revisit its third-party doctrine and to discard it as inconsistent with the property principles of Jones and Jardines.

The Petition should be granted.

Respectfully submitted,

MICHAEL CONNELLY
U.S. JUSTICE FOUNDATION
932 D STREET, STE. 2
Ramona, CA 92065
Attorney for Amicus Curiae U.S. Justice Foundation

**Counsel of Record*
November 3, 2016

HERBERT W. TITUS*
ROBERT J. OLSON
WILLIAM J. OLSON
JOHN S. MILES
JEREMIAH L. MORGAN
WILLIAM J. OLSON, P.C.
370 Maple Ave. W.
Ste. 4
Vienna, VA 22180
(703) 356-5070
wjo@mindspring.com
Attorneys for Amici Curiae