No._____

IN THE SUPREME COURT OF THE UNITED STATES

October Term 2016

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

Corrected Petition for Writ of Certiorari

JAMES G. CONNELL, III
Connell Law, L.L.C.
P.O. Box 141
Cabin John, MD 20818
(703) 623-8410
jconnell@connell-law.com

JAMES WYDA
Federal Public Defender
District Of Maryland
MEGHAN SKELTON
Appellate Attorney
Counsel of Record
6411 Ivy Lane, 7th Floor
Greenbelt, Maryland 20770
(301) 344-0600
meghan_skelton@fd.org

Attorneys for Petitioner

Questions Presented

1. Law enforcement uses cell site location information to track and reconstruct the location and movements of cell phone users over extended periods of time. Does the Fourth Amendment require law enforcement to obtain a warrant to acquire this information?

2. Title 18 U.S.C. § 2703 contains both a provision that requires the government to seek a warrant in order to obtain stored location information from cellular service providers, as well as a provision allowing law enforcement to obtain this data on less than probable cause. Does 18 U.S.C. § 2703 support application of the good-faith exception to law enforcement's acquisition of over seven months of cell site location information without a warrant?

List of Parties

An additional party in the proceeding in the court whose judgment is the subject of this petition is Eric Jordan.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

FEDERAL CASES

STATE CASES

STATUTES

Petition for Writ of Certiorari

Petitioner Aaron Graham respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Fourth Circuit in this case.

Opinions Below

The opinion of the en banc United States Court of Appeals (Pet. App. 1a-66a) is published at 824 F.3d 421 (4th Cir. 2016). An earlier opinion of a three-judge panel of the Fourth Circuit (Pet. App. 67a-200a) is published at 796 F.3d 392 (4th Cir. 2015). The decision of the district court (Pet. App. 201a-240a) is published at 846 F. Supp. 2d 384 (D. Md. 2012).

Jurisdiction

The en banc United States Court of Appeals for the Fourth Circuit issued its opinion and judgment on May 31, 2016. Petitioner requested and was granted a four-week extension of time to file a petition for a writ of certiorari. The jurisdiction of this Court is invoked under 28 U.S.C. § 1254(1).

Constitutional and Statutory Provisions Involved

The Fourth Amendment to the United States Constitution states:

> 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 person or things to be seized.

The Stored Communications Act, 18 U.S.C. § 2703, states in pertinent part:

> **(c) Records concerning electronic communication service or remote computing service.—(1)** A government entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—
>
> > **(A)** obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;
> >
> > **(B)** obtains a court order for such disclosure under subsection (d) of this section; * * *
>
> **(d) Requirements for court order.**—A court order for disclosure under subsection (b) or (c) may be issued by any court of competent jurisdiction and shall issue only if the government entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or other records or other information sought, are relevant and material to an ongoing criminal investigation. * * *

Statement of the Case

Following a jury trial in the United States District Court for the District of Maryland, Aaron Graham was found guilty of conspiracy to violate the Hobbs Act and substantive Hobbs Act robberies, in violation of 18 U.S.C. § 1951; possessing and brandishing a firearm in furtherance of a crime of violence, in violation of 18 U.S.C. § 924(c), and being a felon in possession of a firearm, in violation of 18 U.S.C. § 922(g). He was sentenced to 1,764 months in prison. A divided panel of the Fourth Circuit decided that the government obtained evidence of Mr. Graham's historic cell site location information (CSLI) in violation of the Fourth Amendment. Pet. App. 80a, 85a. The government petitioned for rehearing, and the en banc court reversed the decision of the panel. Pet. App. 4a-5a.

When someone uses a cell phone to make or receive calls, send or receive text messages, run certain apps, or search the internet, the cellular service provider "automatically generates" location information. Pet. App. 109a. Cell phone users do not actively input location in order to use the service. The location data is created "without the user's active participation." Pet. App. 109a. Rather, this location data is "quietly and automatically calculated by the network, without unusual or overt intervention that might be detected by the user." Pet. App. 110a (citations omitted). Moreover, the data is neither tangible nor visible to the user. *Id.* "It is purely a function and product of cellular telephone technology, created by the provider's system network at the time that a cellular telephone call connects to a cell site." *Id.* (citation omitted).

Generally, when connecting to the network, the cell phone connects to the nearest tower. Pet. App. 81a. As a person moves, the cell site can change even during a single call. By tracing different cell sites for a particular phone throughout the day and during individual calls, the government can track a person using a phone over time. *Id.* The proliferation of cellular infrastructure and advances in technology gives service providers and the government "a continuing stream of increasingly precise information about the locations and movements of network users." Pet. App. 122a.

1. After arresting Aaron Graham for two armed robberies of fast food restaurants in Baltimore, local and federal law enforcement began investigating whether he may have been involved in several unsolved robberies. Rather than seeking a search warrant, the government submitted an application to a magistrate

judge for a corporate records subpoena authorized under the SCA, 18 U.S.C. § 2703(d), granting access to 221 days of Mr. Graham's historical location information. Pet. App. 241a-258a. The standard for obtaining court-ordered subpoenas under this statute is lower than probable cause, requiring only "specific and articulable facts showing that there are reasonable grounds to believe that" the cell phone records "are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

Using this subpoena, the government compelled Sprint/Nextel to provide it with Mr. Graham's cellular telephone call detail records for the period between July 1, 2010, and February 6, 2011, or 221 days. JA 2668-3224. The records included the date, time, and duration of each call. They also identified the first and last cell site for each of Mr. Graham's calls, along with the latitude and longitude of each cell site. For some of the calls, the first and last sites were the same, implying that Mr. Graham remained in one place during the call. In others, the sites changed, allowing the government to reconstruct Mr. Graham's movement during the call.

These records included information on 20,036 calls, 14,805 of which included location information. These 14,805 calls showed the government 29,659 location points. This data revealed an average of 134 location points per day, or approximately one location point every 11 minutes for seven months. Taken together, these records allowed the government to create a 221-day surveillance map of Mr. Graham's movements at all times of the day and night, both inside and outside his home.

2. The government charged Mr. Graham and a co-defendant, Eric Jordan, with multiple robbery and firearms counts, in violation of 18 U.S.C. § 1951, § 924(c), and § 922(g). They moved to suppress the call detail records. They argued that using a subpoena, rather than a warrant, to obtain these records was an unreasonable search under the Fourth Amendment because historical cell site location information (CSLI) reveals non-public information about constitutionally protected areas and reveals a wealth of intimate details about the cell phone user's private life over a significant period of time. *See* Mot. To Suppress 3-4, 1:11-cr-00094 Docket Entry 38 (D. Md. July 28, 2011).

The government opposed the motion, on the ground that Mr. Graham did not have an objectively reasonable expectation of privacy in his location information since he had knowingly and voluntarily disclosed it to the cellular service provider by the mere act of carrying a cell phone. It relied on the third-party doctrine set forth in *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976).

The district court agreed that "the implications of law enforcement's use of this historical cell site location data raise the specter of prolonged and constant government surveillance," but nevertheless denied the motion. Pet. App. 209a. Under *Smith* and *Miller*, according to the district court, the petitioner had no objectively reasonable expectation of privacy in location information over time because he had knowingly and voluntarily shared the data with the provider. Pet. App. 229a. Finally, in the alternative, the court decided that suppression was not an available

remedy because the government had relied in good faith on the court order to obtain the data, and that reliance was objectively reasonable. Pet. App. 238a-239a.

At trial, the government plotted Mr. Graham's location at various times relevant to its case on a map that it presented to the jury. It argued to the jury that its surveillance of Mr. Graham, using CSLI, established that he was at the scene of the unsolved robberies. JA 2056-60; 2446, JA 2663-66. The jury convicted Mr. Graham and his co-defendant.

3. A divided panel of the court of appeals reversed the district court's decision but affirmed the convictions. The court of appeals decided that cell phone users enjoy an objectively reasonable expectation of privacy from government surveillance of their movements via historical CSLI. The court decided that law enforcement conducts a search when it inspects this information, and that the government must use a warrant to acquire this information.

The court analogized tracking CSLI to the searches this Court addressed in *United States v. Karo*, 468 U.S. 705 (1984), and *Kyllo v. United States*, 533 U.S. 27 (2001), where this Court required the government to obtain a warrant to learn information that places an individual and her private property in a home. Pet. App. 87a-91a. The court decided that inspecting "long-term CSLI invades an even greater privacy interest than the search challenged in *Karo*" because it allows the government to track a person, potentially placing each Appellant at home on several dozen specific occasions, far more than the single instances discovered in *Karo* and *Kyllo*." Pet. App. 90a. *See also id.* at 99a (describing the tracking here as involving an

"impressive 29,659 location data points . . . amounting to well over 100 data points for each Appellant per day on average.").

The court of appeals rejected the government's argument that people do not enjoy a privacy interest in their location information because the records are kept in the ordinary course of the service provider's business. Pet. App. 102a. "We decline to apply the third-party doctrine in the present case because a cell phone user does not 'convey' CSLI to her service provider at all – voluntarily or otherwise – and therefore does not assume any risk of disclosure to law enforcement." Pet. App. 109a.

The court of appeals thus concluded that the government must use a warrant supported by probable cause in order to acquire and inspect historical CSLI. The court, however, declined to suppress the evidence on the grounds that the government acted in good faith reliance on court orders issued under the SCA. Pet. App. 126a. The court decided that the "constitutionally infirm decision" "was not so clear" because the Fourth Circuit had not yet ruled on the issue. Pet. App. 130a.

4. The Fourth Circuit granted the government's petition for rehearing en banc, and reversed the panel's decision. The divided en banc court decided that *Smith* controls. The court concluded that Mr. Graham had "unquestionably 'exposed' the information at issue to the phone company's equipment in the ordinary course of business," by virtue of his carrying a cellphone. Pet. App. 5a (citations omitted). The court distinguished *Karo, Kyllo,* and *United States v. Jones*, 132 S. Ct. 945 (2012), as well as decisions from several states' supreme courts, stating that the location tracking and tracking into private space was not the issue.

The en banc court noted that its decision that cell phone users voluntarily disclose their location information to the service provider conflicts with a decision from the Third Circuit. Pet. App. 5a. The Third Circuit declined to apply *Smith* to the use of historical CSLI to track an individual's movements and location, reasoning that "a cell phone customer has not voluntarily shared his location with a cellular providers in any meaningful way." *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Service to Disclose Records to Gov't*, 620 F.3d 304, 313 (3d Cir. 2010) (hereinafter *In re Application (Third Circuit)*). The Fourth Circuit, however, reasoned that "cell phone users convey CSLI to their service providers 'voluntarily.'" Pet. App. 6a.

Nevertheless, as the court below also noted, the Third Circuit ultimately concluded that a magistrate judge may issue an order under the SCA based on less than probable cause. Pet. App. 5a. In addition, the court described its application of the third party doctrine as consistent with decisions from the Fifth, Sixth, and Eleventh Circuits.

Reasons for Granting the Petition

This petition raises an unresolved issue of national importance involving the Fourth Amendment implications of the government's use of new technology to track the movements of cell phone users over time. Three times, this Court has noted, but reserved ruling, on issues that this case presents. Presently, there is a doctrinal split between the Third Circuit and the Fourth, Fifth, Sixth, and Eleventh Circuits over whether citizens voluntarily disclose their location for the purpose of government surveillance solely by carrying a cellular phone, which passively connects to a phone

company's service towers. Courts of appeal have split over whether and how to apply this Court's pre-digital Fourth Amendment cases to cell phones. Federal courts of appeals and state courts of last resort have split over whether individuals have a privacy interest in location data.

Tens of thousands of times per year, law enforcement compels cellular service providers to turn over cell phone users' location data.[1] In Florida or New Jersey, whether the government must use a warrant or a subpoena depends on whether the request comes from federal or state agencies. In Pennsylvania and Delaware, this issue is left to a magistrate judge's discretion. In other jurisdictions, federal judges have asked for guidance from this Court, even though they have found that the Fourth Amendment's warrant requirement does not apply.

I. This case presents an important and unresolved question about the application of this Court's pre-digital precedents to new technologies that aggregate location data over time.

Lower courts have divided over how to apply pre-digital Fourth Amendment law to cell site location information. Although this Court has touched on the

---

[1] Prosecutors in the District of the District of Columbia have stated that requests for call detail information, including what the government calls simple "routing" information, quadrupled from 2012 to 2013. *See* Spencer S. Hsu, *A U.S. Judge Just Disclosed How Often Law Enforcement Asked to Secretly Track Electronic Records*, Washington Post, September 21, 2016, available at https://www.washingtonpost.com/local/public-safety/us-judge-lists-one-years-government-electronic-surveillance-requests-in-dc/2016/09/21/7911b044-7c26-11e6-beac-57a4a412e93a_story.html. This government "surveillance method[] coupled with computing and storage capabilities enable[s] authorities to use laws that date to a copper-wire and telephone exchange world to sweep up vast amounts of digital data to map much of a person's movement and social relationships without a search warrant." *Id.*

intersection of new technology and pre-digital law, this case presents the unsettled issue of privacy and property interests in aggregated location data, as well as the continuing viability of the third party doctrine in a society in which unprecedented quantities of sensitive, private information is held by a third party.

Lacking definitive guidance from this Court, lower courts have struggled to find the correct analogy for the government's use of CSLI to track citizens' locations and movements over time. Is CSLI like a dialed telephone number? Is it like a beeper following property into a constitutionally protected space? Or is it something new which requires re-thinking older Fourth Amendment doctrines? Following ten years of the Magistrate's Revolt and mature Circuit Court consideration, this case presents an ideal vehicle for the Court to explain the meaning of the Fourth Amendment in the digital age.

A. Mobile phone technology, including the use of passively generated CSLI, has outstripped the reasoning of *Smith* and *Miller*.

In this case, as it has done tens of thousands of times, the government used a subpoena to obtain a spreadsheet which surveilled—within a margin of error—the defendant's location an average of every eleven minutes for seven months. Such comprehensive and easily-obtained location tracking threatens to fundamentally alter the relationship between the government and the governed. The lower courts need guidance, because their analogies between the advanced, networked hand-held computers called "cell phones" and pre-digital technologies like landlines and deposit logs have strained beyond the breaking point.

The technological starting point for the Fourth Amendment is the human eye,

as "visual observation is no 'search' at all." *Kyllo*, 533 U.S. at 32; *see also Boyd v. United States*, 116 U.S. 616, 628 (1886). This Court has allowed, without a warrant, relatively minor extensions of human capabilities, including police use of telescopes, flyovers at a reasonable distance, and electronic tracking via beepers for short periods of time on public roads. *See Florida v. Riley*, 488 U.S. 445 (1989); *Dow Chemical v. United States*, 476 U.S. 227, 234-35 (1986); *California v. Ciraolo*, 476 U.S. 207, 213 (1986); *United States v. Knotts*, 460 U.S. 276 (1983). In *Smith*, the case on which the court below relied most heavily, this Court highlighted the "limited capabilities" of a pen register to replace a human switchboard operator. 442 U.S. at 741-42.

The question "how much technological enhancement of ordinary perception . . . is too much" remains unanswered. *Kyllo*, 533 U.S. at 33. Yet the Fourth Amendment requires a determination of "what limits there are upon this power of technology to shrink the realm of guaranteed privacy." *Id.* The current technological environment has infiltrated and altered the legal landscape. This Court has criticized a "mechanical application" of search and seizure law decided decades ago when faced with data searches like the one that occurred here. *Riley v. California*, 134 S. Ct. 2473, 2484 (2014). Cases decided in the 1970s simply do not address current reality.

Cell phones are qualitatively different from the technology considered in *Smith*. "The term 'cell phone' is itself misleading; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone." *Riley*, 134 S. Ct. at 2489. The location tracking technology the government exploited

here was "nearly inconceivable just a few decades ago, when *Chimel* and *Robinson*"—as well as *Smith* and *Miller*—"were decided." *Id.*

In 1986, when Congress enacted the Electronic Communications Privacy Act, which includes the SCA at issue here, what is now routine was the stuff of science fiction. Mobile phones had only been commercially available for two years, at a cost approaching $4,000 per handset. The technological capacity to monitor and store location information for wireless calls would not even exist for about ten years, when the government and telecommunications providers entered into a joint protocol to develop and deploy hardware and software that enabled law enforcement to track people's location using their cell phones.[2]

A modern cell phone is not a telephone in any sense that this Court would have recognized in 1979, when it considered in *Smith* what happens when a person dials a land-line phone. Treating the smartphones and their capabilities at issue in this case like a copper-wire phone "is like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Riley*, 134 S. Ct. at 2488.

Because people carry their cell phones on their person, CSLI implicates privacy issues far beyond any location tracking case this Court has yet considered. Cell phones are only useful when carried in close proximity to their users, meaning that the location of a cell phone is a near-perfect proxy for the location of a person.

---

[2] *See* FCC Order No. 98-223 at 6; *In The Matter of Petition For an Extension of the Compliance Date Under Section 107 of the Communications Assistance for law Enforcement Act*, (September 11, 1998); Statement of Thomas J. Sugrue, Chief, Wireless Telecommunications Bureau, FCC, Subcommittee on Telecommunications Trade, and Consumer Protections, H.R. Commerce Comm. Hrg., June 14, 2001 (http://transition.fcc.gov/Speeches/misc/statements/sugrue061401.pdf).

"According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower." *Id.* at 2490. Cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Id.* at 2484.

Detailed, aggregated location tracking created by CSLI is a current reality. As the record demonstrates, "cell phones and other wireless devices now permit wireless carriers to track and record the location of users." *Jones*, 132 S. Ct. at 963 (Alito, J., concurring). The use of CSLI monitoring is not materially different from GPS,[3] insofar as it "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id.* at 955 (Sotomayor, J., concurring). "Historic location information . . . can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." *Riley*, 134 S. Ct. at 2490.

Although the information collected from *Smith's* land-line pen register, the only type of telephone service available to Americans in 1979, implies that someone is inside a particular building when a call is dialed or answered, this apparent similarity to CSLI's ability to locate people in private space is superficial at best. A pen register is stationary, so it does not invoke the location tracking privacy interests

---

[3] "GPS data and historical CSLI are linked at a fundamental level" because they both track an individual's movements over time. *Commonwealth v. Augustine*, 4 N.E.3d 846, 866 (Mass. 2014).

that the Court considered in *Riley* and *Jones*—but not in *Smith*.

A pen register provides the government with a list of numbers dialed and the time when the call occurred. Unlike CSLI, a dialed phone number is associated with a place, not a person. And it does not reveal who was calling, who was with the caller, whether the caller was moving or staying in one place. Indeed, the limited information revealed by a pen register was central to the decision in *Smith*. 442 U.S. at 742. "Neither the purport of any communication between the caller and recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers." *Id.* at 741 (internal quotation omitted).

CSLI, unlike dialed telephone numbers, is more than pure routing information. As various state courts have found, "CSLI clearly has the potential to track a cellular telephone user's location in constitutionally protected areas." *Augustine*, 4 N.E.3d at 864. *See also State v. Earls*, 70 A.3d 630, 642 (N.J. 2013) ("Modern cell phones also blur the historical distinction between public and private areas because cell phones emit signals from both places."). And "in the home . . . all details are intimate details, because the entire area is held safe from prying government eyes." *Kyllo*, 533 U.S. at 37. When the government uses technology "to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." *Id.* at 40.

Law enforcement cannot replicate tracking a person by CSLI in a non-digital way. Analyzing historic CSLI allows the government to reconstruct history. With

CSLI, the government can turn back the clock to surveil a suspect's location and movements when the suspect was not yet even a suspect, and perhaps when no investigation was under way—before a crime may have been contemplated, let alone committed. Even if a constable hiding in a carriage could approximate GPS surveillance, no possible analog exists for the use of historic CSLI. *Cf. Jones*, 132 S. Ct. at 958 (Alito, J., concurring). Here, the government literally could not have tracked the petitioner without CSLI technology; it relied on the ability to "store such records and efficiently mine them for years to come." *Id.* at 955-56 (Sotomayor, J., concurring).

Moreover, because monitoring CSLI, like GPS, "is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: limited police resources and community hostility." *Id.* at 956 (Sotomayor, J., concurring). The Government's current and increasing "power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of information about any person whom the Government, in its unfettered discretion, chooses to track—may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'" *Id.* (Sotomayor, J., concurring) (quoting *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

Modernizing decades-old search and seizure law to technology like this is sound and overdue. Historic CSLI bears as much resemblance to a pen register as

Riley's moon shot and horseback ride.

B. This Court should grant certiorari to reconsider the reasonable expectation of privacy and third-party principles from *Katz*, *Smith*, and *Miller*.

The increasing threat of technology to privacy highlights the weakness of the test based on subjective and societal beliefs about what privacy people do and do not enjoy. "The *Katz* test—whether the individual has an expectation of privacy that society is prepared to recognize as reasonable—has often been criticized as circular, and hence subjective and unpredictable." *Kyllo*, 533 U.S. at 34; *see also Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). As Justice Alito noted, this test "is not without its own difficulties. It involves a degree of circularity, and judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks." *Jones*, 132 S. Ct. at 962 (Alito, J., concurring) (citations omitted).

Smith itself imagined a situation like that confronting the Court today, in which the reasonable expectation of privacy test may be insufficient to protect constitutional values. *Smith* observed that the *Katz* test could "provide an inadequate index of Fourth Amendment protection. For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects." 442 U.S. at 741 n.5.

Twice in recent years, this Court has identified a problematic intersection between government access to digital information held in a third party's hands. In

her *Jones* concurrence, Justice Sotomayor commented, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring). She criticized the doctrine as "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." *Id.* at 957 (Sotomayor, J., concurring). The Court, however, did not reach the issue, having relied on a more narrow ground to find a Fourth Amendment violation.

Two years later, in *Riley*, when the government argued that *Smith* permitted the warrantless inspection of call logs found on a cell phone, this Court declined to engage in the debate. The Court stated that, since the government had conceded that it had "searched" the defendants' cell phones, it need not address whether a Fourth Amendment search had occurred—which was the central issue in *Smith*. *Riley*, 134 S. Ct. at 2492-93. Nevertheless, the Court commented that the information available in a cell phone's call log was not analogous to the limited information available from a pen register. *Id.* at 2493.

The all-or-nothing approach to privacy in *Smith* and *Miller* is even more dissonant with the digital age. These cases, relied on by the Fourth Circuit, reasoned "that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, 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." *Miller*, 425

U.S. at 443. It is questionable whether such a binary approach should apply to a pervasive technology like cell phones. Even if the absolute, binary approach to privacy made sense in the 1970s, it should not govern modern electronic communication. As Justice Harlan might have said, "bad physics" makes "bad law, for reasonable expectations of privacy may be defeated by electronic as well as physical invasion." *Katz*, 389 U.S. at 361 (1967) (Harlan, J., concurring).

In the digital age, telephone and cable companies, internet service providers, and app developers are enablers rather than recipients of private communications. Many forms of modern electronic communication belie the legal fiction that sharing data with intended recipients is the same as sharing it with the world. Facebook, Instagram, and LinkedIn all allow a user to control which other users can view her data. Snapchat and Wickr limit the amount of time even an intended recipient can view a user's data. Yet the Fourth Circuit's interpretation of Fourth Amendment law treats a private photograph shared only with a spouse on Snapchat for a limited time as the equivalent of a billboard on a busy highway, open to view by all who drive by.

Multiple opinions in the numerous CSLI cases have commented on the poor fit between the third party doctrine and the government's acquisition and analysis of detailed, intimate location information revealed in CSLI. The Fourth Circuit noted that "although 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."

Pet. App. 36a. *See also United States v. Davis*, 785 F.3d 498, 521-22 (11th Cir. 2015) (Jordan, concurring) ("I have some concerns about the government being able to conduct 24/7 electronic tracking (live or historical) in the years to come without an appropriate judicial order. And I do not think I am alone in this respect."); *Tracey v. State*, 152 So. 2d 504, 529 (Fla. 2014) (Polston, J., concurring) (suggesting that if the third party doctrine were to eliminate a privacy interest in the location information collected by CSLI, "we may be facing a situation in which *Katz's* two-pronged inquiry [provides] an inadequate index of Fourth Amendment protection.") Both the New Jersey and Massachusetts Supreme Courts have expressed that *Smith* and *Miller* fail to protect the personal privacy invaded by long term location tracking via CSLI. *Earls*, 70 A.3d at 641; *Augustine*, 4 N.E.3d at 243-45.

Not only have the lower courts debated how to apply the third party doctrine correctly, but they have also struggled with choosing among competing Fourth Amendment doctrines. "After all, *Jones* held that the *Katz* formula is but one way to determine if a constitutionally qualifying 'search' has taken place." *United States v. Ackerman*, __ F.3d __, 2016 WL 4158217 *11 (10th Cir. Aug. 5, 2016). Since a search occurs when the government physically intrudes on constitutionally protected space, persons, houses, papers, or effects in order to learn information, "the fact that the government's conduct doesn't trigger *Katz* doesn't mean it doesn't trigger the Fourth Amendment." *Id.*

The Fourth Circuit squarely rejected any application of the *Jones* trespass test. Pet. App. 9a. The Fourth Circuit found irrelevant whether individuals have a

property interest in their data or their location, exclusively considering the *Katz* test as expanded in *Smith* and *Miller*. *See* Pet. App. 9a, 11a.

The Tenth Circuit, however, recently embraced it in the context of searching data. That court described the government's warrantless examination of the defendant's data as "pretty clearly" the exact "type of trespass to chattels that the framers sought to prevent when they adopted the Fourth Amendment." *Ackerman*, 2016 WL 4158217 at *11.

Personally identifying information, like a person's location and movements over time, constitutes modern "papers and effects." This data, particularly when aggregated, comprises a thing uniquely identified with and of value to a specific person.[4] Courts, however, have had difficulty in applying *Jones* and the notion of governmental trespass on digital property. This property, however, is every bit as susceptible to governmental intrusion as a car, home, or desk.

II. Lower courts and law enforcement currently lack guidance on issues they confront daily.

Lacking guidance from this Court, the state of the law regarding law enforcement's ability to track an individual's movement and location via CSLI is fractured. Although the federal circuits have not split in *result*, they have split in reasoning. And they have struggled with how to resolve the Fourth Amendment implications of the internally contradictory SCA, the third party doctrine, and

---

[4] *See, e.g.*, World Economic Forum, *Personal Data: An Emerging New Asset Class*, (http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf) (January 2011).

constitutional protections of privacy and property. The six principal federal cases on this issue have resulted in 17 different opinions and direct conflicts with state courts, leaving doctrinal uncertainty and a patchwork of applicable standards across jurisdictions.[5] *See* Pet. App. 47a-48a n.2.

A. The Circuit Courts and state courts of last resort have split in reasoning, and in some cases result.

1. The Circuits and sovereigns have split over whether the third party doctrine eliminates an individual's reasonable expectation of privacy in historical CSLI.

An open and acknowledged split exists regarding whether the third party doctrine of *Smith* and *Miller* eliminates an individual's privacy interest in the movement and location information captured by CSLI. Courts have intractably divided over whether people knowingly and voluntarily expose their movements to their cellular service providers by virtue of carrying a cell phone. The Fourth, Fifth, Sixth and Eleventh Circuits have decided that the third party doctrine applies to CSLI surveillance, rendering it ungoverned by the Fourth Amendment. The Third Circuit, Florida Supreme Court, and Indiana Court of Appeals have decided the opposite.

The Fourth Circuit held, "Defendants unquestionably 'exposed' the information at issue to the phone company's 'equipment in the ordinary course of

---

[5] In addition to the census of opinions that Judge Wynn catalogued in dissent in the court below, this case itself has resulted in six different opinions. Judge Wynn also did not include an additional CSLI case from the Fifth Circuit, *United States v. Guerrero*, 768 F.3d 351 (5th Cir. 2014).

business.'" Pet. App. 12a (quoting *Smith*, 442 U.S. at 744). The court further held that cell phone users convey their location data voluntarily: "A cell phone user voluntarily enters an arrangements with his service provider in which he knows that he must maintain proximity to the provider's cell towers in order for his phone to function." Pet. App. 18a. The court noted that "some cell phone users may not recognize, in the moment, that they are 'conveying' CSLI to their service provider," but decided that *Smith* and *Miller* "do not require contemporaneous recognition of every detail an individual conveys to a third party" – as long as "an individual does not *in*voluntarily convey[] information." Pet. App. 18a-19a (emphasis supplied).

The Fifth Circuit reached a similar conclusion because citizens' "use of their phones . . . is entirely voluntary . . . . The government does not require a member of the public to own or carry a phone." *In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600, 613 (5th Cir 2013) (hereinafter *In re Application (Fifth Circuit)*). As did the Eleventh and Sixth Circuits. *Davis*, 785 F.3d at 511; *United States v. Carpenter*, 819 F.3d 880, 888 (6th Cir. 2016).

The Third Circuit, however, reached the opposite conclusion. "A cell phone user has not 'voluntarily' conveyed his location information with a cellular provider in any meaningful way." *In re Application (Third Circuit)*, 620 F.3d at 317. First expressing skepticism that cell phone users understand how CSLI is generated and stored, the court then found that when people place a cell phone call, "the only information that is voluntarily conveyed to the phone company is the number that is dialed." *Id.* (internal quotation omitted). Moreover, that court noted that, when cell

phone users receive a call, they haven't "voluntarily exposed anything at all." *Id.*

Two states have reached the same result as the Third Circuit, though they have further concluded that a warrant is required to use CSLI. The Florida Supreme Court held that *Smith* and *Miller* do not erase a reasonable expectation of privacy in CSLI. Applying the "normative inquiry envisioned in *Smith*," the court decided that the cell phone user "did not voluntarily convey [CSLI] to the service provider for any purpose other than to enable use of his cell phone for its intended purpose." *Tracey*, 152 So. 3d at 525-26.

The Florida Supreme Court reasoned, "Simply because the cell phone user knows or should know that his cell phone gives off signals that enable the service provider to detect its location for call routing purposes," does not amount to assuming the risk that the service provider will share or use the location data for any other purpose. *Id.* at 522. The court likewise rejected the notion that using a cell phone amounts to consent to be tracked or voluntarily disclosing location: "Requiring a cell phone user to turn off the cell phone just to assure privacy from governmental intrusion that can reveal a detailed and intimate picture of the user's life places an unreasonable burden on the user to forego necessary use of his cell phone, a device now considered essential by much of the populace." *Id.*

The Indiana Court of Appeals agreed with the Third Circuit and Florida court. "We decline to apply the third-party doctrine in the present case because a cell phone user does not convey historical location data to his provider at all—voluntarily or otherwise—and therefore does not assume any risk of disclosure to law enforcement."

Zanders v. State, __ N.E.3d __, 2016 WL 4140998 *8 (Ind. App. Aug. 4, 2016). The court explained that cell phone users do not affirmatively enter their location when they make a call, but that CSLI is "rather quietly and automatically calculated by the network, without unusual or overt intervention that might be detected by the target user." *Id.* (internal quotation omitted). Moreover, rejecting the reasoning of the Fourth and Fifth Circuits, the court stated, "A cell phone user's understanding of how cellular networks generally function is beside the point. The more pertinent question is whether a user is generally aware of what specific cell-sites are utilized when their phone connects to the network." *Id.* at *9.

The Texas Court of Criminal Appeals has adopted an ambiguous position in this split. *See Ford v. State*, 477 S.W.3d 321 (Tex. Crim. App. 2015). That court noted both the existence of the split and the tension between the third party doctrine permitting CSLI tracking with the concurring opinions in *Jones*. *Id.* at 335. The court stated, "Nevertheless, we are confident that the discrete four days of location data at issue in this case—which did not reveal a comprehensive view of the specific details of appellant's daily life—falls squarely inside the third-party-doctrine ball-park." *Id.* The court left open the possibility that the result could change if the tracking is more extensive. *Id.* at 334 ("We acknowledge that Fourth Amendment concerns might be raised if long-term location information were acquired.").

2. The Circuits and the sovereigns have split over on the question of a privacy interest in location data over time.

This case also involves a related split on whether individuals enjoy a privacy interest in long-term location tracking. The Fourth Circuit rejected the notion that

individuals have a privacy interest in long-term location monitoring, deciding that the availability of information about an individual's location to third parties destroys any expectation of privacy. Pet. App. 29a-32a. "We recognize the appeal—if we were writing on a clean slate—in holding that individuals *always* have a reasonable expectation of privacy in large quantities of location information, even if they have shared that information with a phone company. But the third-party doctrine does not afford us that option." Pet. App. 32a. The Eleventh Circuit agrees. "Reasonable expectations of privacy do not turn on the quantity of non-content information MetroPCS collected in its historical cell tower location records." *Davis*, 785 F.3d at 515.

The District of Columbia Circuit, however, recognizes a reasonable expectation of privacy interest in long-term location information, even if the public or third parties can observe a person's movements. In *United States v. Maynard*, the D.C. Circuit explained the privacy implications of long-term location monitoring. "Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation." 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd on other grounds sub nom. United States v. Jones*, 132 S. Ct. 945 (2011). Surveilling a person's movements over time reveals whether the person "is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or

political groups—and not just one such fact about a person, but all such facts." *Id.* Monitoring the defendant's movements over time, albeit on public roads, constituted a search subject to the Fourth Amendment's warrant requirement. *Id.*

Multiple state supreme courts have reached the same conclusion as the D.C. Circuit, and the opposite conclusion of the court below. For example, the Court of Appeals of New York held that "constant, relentless tracking" reveals "not simply where we go, but by easy inference, of our associations—political, religious, amicable and amorous, to name only a few—and of the pattern of our professional and avocational pursuits." *People v. Weaver*, 909 N.E.2d 1195, 1199-1200 (N.Y. 2009). The Indiana courts explain "the expectation of privacy in one's whereabouts is not only due to society's impulse to cringe at the idea of being followed day and night; the personal nature of the information itself gives rise to an expectation of privacy." *Wertz v. State*, 41 N.E.3d 276, 285 (Ind. Ct. App. 2015), *trans. to Indiana Supreme Court denied*.

Although *Maynard*, *Weaver,* and *Wertz* arose in the context of GPS monitoring, this Court used the same principles, citing to Justice Sotomayor's concurrence in *Jones*, to explain that the use of historical CSLI to reconstruct an individual's movement over time implicates the same interest in long-term location monitoring. Monitoring someone's movements over time reveals a wealth of intimate information providing "a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Riley*, 134 S. Ct. at 2490. This Court used historical location

information as one of the examples of the "privacies of life" revealed through searching cell phones. *Id.*

Other state supreme courts agree that individuals have a reasonable expectation of privacy in the information historic CSLI collectively reveals. Recognizing that CSLI allows the government to track a person beyond simply movement on public roads, the Florida, New Jersey, and Massachusetts Supreme Courts have all found that long-term location monitoring implicates an individual's privacy interests. *Tracey*, 152 So. 2d at 525; *Augustine*, 4 N.E.3d at 864; *Earls*, 70 A.3d at 642; *see also Zanders*, 2016 WL 4140998 at *12.

B. The magistrate judges who regularly confront government requests to search CSLI and related digital media are in sharp disagreement and need guidance.

The government's aggressive pursuit of highly personal digital information using a court order rather than a warrant has sparked what has become known as "the Magistrate's Revolt." The first published decision[6] in the Magistrate's Revolt denied the government's request for CSLI with a court order rather than a warrant, and "revealed that the Justice Department had routinely been using a baseless legal argument to get secret location tracking authorizations from courts, probably for many years." Jennifer Granick, *Let the Sun Shine In: WaPo Story on the Magistrates'*

---

[6] *In the Matter of an Application of the United States for an Order (1) Authorizing the use of a Pen Register and a Trap and Trace device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information*, 384 F. Supp. 2d 562 (E.D.N.Y. 2005).

Revolt, April 25, 2014.[7] Until this time, "magistrate judges with only a DOJ lawyer in front of them would often misplace their faith in government assertions of investigatory power and the relative scope of individual privacy rights." *Id.* Increasingly, "Judges at the lowest levels of the federal judiciary are balking at sweeping requests by law enforcement officials for cellphone and other sensitive personal data, declaring the demands overly broad and at odds with basic constitutional rights." Ann E. Marimow and Craig Timberg, *Low-Level Federal Judges Balking at Law Enforcement Requests for Electronic Evidence*, Washington Post, April 24, 2014.[8]

A trend has arisen involving a series of magistrate judges, "the work horses of the federal courts," who have started denying requests to obtain "all encompassing, swaths of electronic communications of suspects." Patrick J. Cotter, *The Magistrate's Revolt: Unexpected Resistance to Federal Government Efforts to get General Warrants for Electronic Information*, The National Law Review (May 15, 2014).[9] This "revolt" has occurred as a result of the government's repeated requests "to telecommunications companies to provide either large amounts of citizens' emails or even, on a number of occasions, access to detailed location information contained in citizens' cell phones." *Id.*

---

[7] https://www.justsecurity.org/9873/wapo-story-magistrates-revolt/.

[8] https://www.washingtonpost.com/local/crime/low-level-federal-judges-balking-at-law-enforcement-requests-for-electronic-evidence/2014/04/24/eec81748-c01b-11e3-b195-dd0c1174052c_story.html.

[9] http://www.natlawreview.com/article/magistrates-revolt-unexpected-resistance-to-federal-government-efforts-to-get-genera.

Although "published opinions by magistrate judges are relatively rare, . . . legal experts say the overall level of skepticism from magistrates is on the rise." Marimow, *supra.* The Magistrate's Revolt is about ten years old now, "but it has gained power amid mounting public anger about government surveillance capabilities revealed by former National Security Agency contractor Edward Snowden." *Id.* "These court opinions were the first time that the public really began to understand that, although there are federal statutes regulating electronic surveillance by law enforcement, the government—in secret *ex parte* proceedings before magistrate judges across the country—often reaches beyond the authority given to it by law." Grannick, *supra.* Nevertheless, judges charged with the day-to-day oversight of government search practices reach divergent results when reviewing applications for CSLI.[10]

The Magistrate's Revolt demonstrates that "this debate is far from academic." *Id.* Instead, it reveals "that these critical decisions continue to be made every day, in secret, and that a[] small but increasing number of magistrate judges . . . are working hard to surface these issues so that they may be debated and resolved with the full benefit of open judicial scrutiny and public debate." *Id.*

C. The Stored Communications Act is too ambiguous to clarify these issues.

The SCA, 18 U.S.C. § 2703, is ambiguous in its authorization to conduct a

---

[10] *See, e.g., In re Application for Telephone Information Needed for a Criminal Investigation*, 110 F. Supp. 3d 1011 (N.D. Cal. 2015); *United States v. Lang*, 78 F. Supp. 3d 830 (N.D. Ill. 2015); *In the Matter of an Application of the United States for an Order Authorizing the Release of Historical Cell-Site Information*, 736 F. Supp. 2d 578 (E.D.N.Y. 2010).

warrantless search. A statute that purports to authorize a warrantless search must establish certainty and regularity in its application, or it will fail to provide a constitutionally adequate substitute for a warrant. *Illinois v. Krull*, 480 U.S. 340, 358 (1987) (relying on *Donovan v. Dewey*, 452 U.S. 594, 603 (1981)).

The SCA identifies two conflicting, contradictory means for the government to obtain CSLI: when "the government entity—(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . ; [or] (B) obtains a court order for such disclosure under subsection (d) of this section." 18 U.S.C. § 2703(c)(1). The SCA states that the government "can proceed to obtain the records pertaining to a subscriber by several routes, one being a warrant with its underlying requirement of probable cause, and the second being an order under § 2703(d). There is an inherent contradiction in the statute, or at least an underlying omission." *In re Application (Third Circuit)*, 620 F.3d at 319.

Moreover, the statute offers no guidance as to when one section or the other should apply. The ambiguity and contradictions within the statute that the government uses to reach this highly sensitive data fails to offer necessary guidance to courts.

D. This case presents issues considered, but left unresolved in *Jones*, *Riley*, and *Knotts*.

This case allows for the Court to address the issue of long-term monitoring that it reserved in *Jones*. The *Jones* majority stated,

> Thus, even assuming that the concurrence is correct to say that '[t]raditional surveillance' of Jones for a four-week period 'would have required a large team of agents, multiple vehicles, and perhaps aerial assistance,' our cases suggest that such visual observation is

> constitutionally permissible. It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.

132 S. Ct. at 953-54. Since the physical intrusion that occurred in *Jones* supplied a narrow basis for the Court to resolve the Fourth Amendment question, the Court did not need to reach the issue presented here.

Justice Sotomayor's concurrence noted the critical importance of the unresolved question of electronic location monitoring without a trespass. "With increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting . . . GPS-enabled smartphones. In cases of electronic or other novel modes of surveillance that do not depend on a physical invasion of privacy, the majority opinion's trespassory test may provide little guidance." *Id.* at 955 (Sotomayor, J., concurring); *see also id.* at 961 (Alito, J., concurring) ("By contrast, if long-term monitoring can be accomplished without committing a technical trespass—suppose for example, that the Federal Government required or persuaded auto manufacturers to include a GPS tracking device in every car—the Court's theory would provide no protection.").

Justice Alito, on the other hand, saw the "long term monitoring" of Jones's vehicle, independent of the trespass, as the core issue in the case. *Id.* at 958. "The *use* of a GPS for the purpose of long-term tracking" was the "really important" issue. *Id.* at 961 (Alito, J., concurring). Justice Alito, joined by three other justices, would have resolved the case on the basis that long-term monitoring violated a reasonable expectation of privacy. *Id.* at 964 (Alito, J., concurring).

The issue that the Court reserved in *Jones* resurfaced in *Riley*. The unanimous Court in *Riley* noted, but did not need to address, "the question whether the collection or inspection of aggregated digital information amounts to a search." 134 S. Ct. at 2489 n.1.

Although the technology at issue here, as well as in *Jones*, was unimaginable thirty years ago, the possibility of constant surveillance was nonetheless of concern to the Court even then. In *Knotts*, this Court noted the scenario of twenty-four hour surveillance of the defendant. 460 U.S. at 283. Distinguishing the facts of *Knotts*, the Court stated, "if such dragnet type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." *Id.* at 284.

Technological innovation has brought those practices into daily use. This case presents just the dragnet surveillance that the Court refrained from addressing in *Knotts*. The increasing frequency with which these issues arise signals that the time has come for the Court to confront constant surveillance of cell phone users' movements.

III. This case presents an ideal vehicle to resolve the questions presented because it arose in an adversarial context, with a well-developed factual record and extensive judicial consideration.

This case presents an ideal vehicle to resolve the questions presented. Unlike many CSLI cases, this case arose in a fully adversarial context and received en banc consideration below. In addition, the factual record is unusually well developed. The CSLI data itself is part of the public trial record, as are the § 2703(d) orders. These

orders are plainly devoid of probable cause, allowing the Court to consider the substantive differences between the standards addressed in the SCA.[11] There are no disputes of material fact and no procedural obstacles impede consideration of the critical issues in this case.

The 221 days of Mr. Graham's highly personal movement and location information reflected in the record will allow this Court to articulate principles rather than engage in line drawing. The concurrence in *Jones* explained that it "need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark." 132 S. Ct. at 964 (Alito. J., concurring). The Opinion of the Court responded with hypotheticals ranging from "a two-day monitoring of a suspected purveyor of stolen electronics" to "a six-month monitoring of a suspected terrorist." *Id.* at 954. The seven months of tracking in this case exceed any previous benchmark, and indeed exceed the duration of tracking in any other reported CSLI case.[12] The record here is such that this Court can decide the issue with a bright line, rather than reach a fact-dependent solution.[13]

---

[11] This is not always the case. For example, in *Davis*, the applications for the court orders detailed a substantial investigation into the defendant's movements, including statements from cooperating witnesses and forensic evidence, like DNA, already located at the scenes of the crimes under investigation. Petition for a Writ of Certiorari at Appendix 144a-146a, *Davis v. United States*, S. Ct. No 15-146 (July 30, 2015).

[12] In *Carpenter*, the government obtained 127 days of CSLI for one defendant and 88 days of CSLI for the other. 819 F.3d at 886. The Fifth and Eleventh Circuits considered two months of CSLI. *See Davis*, 785 F.3d at 502; *In re Application (Fifth Circuit)*, 724 F.3d at 602. *Zanders* addresses 30 days of CSLI. 2016 WL 4140998 * 2

[13] States have already found themselves attempting to formulate a line. *See Ford*,

See Riley, 134 S. Ct. at 2497 ("Law enforcement officers need clear rules").

Finally, commentators have focused attention on this case as presenting critical issues that this Court should resolve. *See, e.g., Warrantless Seizure of Mobile Phone Data Violates Fourth Amendment, Ind. Court Rules*, 99 Crim. L. Rep. 621 (Aug. 17, 2016) (comparing this case to *Zanders*). If this Court is so inclined, this case allows reconsideration of the "reasonable expectation of privacy" test in present-day where the carrying of a cellular phone and other similar technology is not only a mundane part of daily life for most citizens, but a necessary one.

IV. This Court should grant certiorari to resolve an important question regarding the good faith exception that this Court left open in *Davis v. United States* and that has split the Circuits and highest courts of several states.

The Court should also review the decision of the court below that the government relied in good faith on the subpoena. The Fourth Circuit equated relying on the court order, issued on a standard of less than probable cause, with relying on a search warrant. Pet. App. 129a-131a. *See United States v. Leon*, 468 U.S. 897 (1984). This decision raises an important and recurring question, conflicts with decisions of this Court, and implicates a related conflict with decisions of other lower courts.

This issue is of national importance: what constitutes reasonable law

---

477 S.W.3d at 335 (deciding that seizing and searching "the discrete four days of location data at issue in this case—which did not reveal a comprehensive view of the details of appellant's daily life" did not violate the Fourth Amendment, but suggesting the result could be different if a different factual scenario presented itself). The Massachusetts Supreme Court has found that tracking fourteen days of historical CSLI impermissibly intrudes on a right of privacy, but tracking for a period of six hours does not. *Compare Augustine*, 4 N.E.3d at 855, *with Commonwealth v. Estabrook*, 38 N.E.3d 231, 238 (Mass. 2015).

enforcement reliance on cases, statutes, and principles created or decided when the particular law enforcement practice was never contemplated. This question will repeatedly face courts reviewing the government's attempts to extend old law to new science.

The judgment below raises the question that this Court left unresolved in *Davis v. United States*, 564 U.S. 229 (2011). In *Davis*, this Court decided that suppressing evidence obtained in violation of the Fourth Amendment is not warranted when law enforcement relies on binding appellate precedent that explicitly authorized the particular police practice in question, even if that settled law is later overturned. *Id.* at 241. *Davis*, however, did not reach "the markedly different question whether the exclusionary rule applies when the law governing the constitutionality of a particular search is unsettled." *Id.* at 250 (Sotomayor, J., concurring).

This case presents that open issue. The court below noted that "at the time the government obtained the CSLI at issue here, court rulings outside of this Circuit were in conflict as to the constitutionality of obtaining this information without a warrant." Pet. App. 131a. But the court decided that, since "there was no decisional authority in this Circuit suggesting that the choice presented in § 2703(c) was unconstitutional as applied to CSLI from cell phone service providers[] . . . the government reasonably relied on the SCA in exercising its option to seek a § 2703(d) order rather than a warrant." *Id.* Thus, although recognizing that lower courts had already divided on whether that statute violated the Fourth Amendment, the fact

that the Fourth Circuit itself had *not yet* weighed in on the ongoing debate entitled the government to err on the side of its desired outcome and against the privacy rights of citizens, with no repercussions for guessing wrong in the constitutional debate. *Id. See also United States v. Davis*, 690 F.3d 226, 256 (4th Cir. 2012).

This decision conflicts with *Leon*. The court below cites *Leon* for the proposition that law enforcement may rely in good faith on a warrant "or other court order." Pet. App. 127a. But *Leon* applies specifically "to searches conducted pursuant to warrants." 468 U.S. at 924. It does so because the government presumably and demonstrably acts with good faith when it does the right thing when it meets the constitutional requirement that it seek a warrant supported by probable cause. The same cannot be said when the government actively attempts to exploit a loophole in the warrant requirement in order to avoid meeting the rigors of probable cause.

Leon is clear about this. "[R]eviewing courts *will not* defer to a warrant based on an affidavit that does not 'provide the magistrate with a substantial basis for determining the existence of probable cause.'" *Id.* at 915 (quoting *Illinois v. Gates*, 462 U.S. 213, 239 (1983)) (emphasis added). Reviewing courts thus cannot use *Leon* as a basis to defer to orders that are not based on probable cause, particularly when the officer who sought the order, and conducts the search, knowingly circumvented the safeguards of the warrant requirement and the burden to demonstrate probable cause. *Leon's* prerequisite for the good faith exception is an objective belief that the document the police officer receives from the magistrate is a technically sufficient warrant based on probable cause. *Id.* at 922-23.

Leon explains that police officers who obtain a warrant that appears to satisfy the probable cause requirement can "literally" do "nothing more . . . in seeking to comply with the law." *Id.* at 921 (internal quotation omitted). Suppressing evidence after a police officer conducts a search with a warrant in hand will not serve the exclusionary rule's deterrent effect because suppression would not "alter the behavior of individual law enforcement officers or the policies of their departments." *Id.* at 918. The Fourth Circuit's contrary conclusion misapplies *Leon* to the point of creating a direct conflict with this Court's precedent.

Here, in contrast, law enforcement easily could, but chose not to, follow the constitutionally secure path. They could have followed 18 U.S.C. § 2703(c)'s explicit warrant requirement, which clearly satisfies the Fourth Amendment, instead of taking their chances with the non-warrant procedure of § 2703(d). Unlike *Leon*, the prosecutor who sought and used the § 2703(d) order *knew* that the order was neither a warrant nor the equivalent of a warrant, and knew that the constitutionality of his choice was already in doubt.

Indeed, suppressing the evidence here *would* alter the behavior of both individual officers and policies of departments and thus would serve the deterrent purposes of the exclusionary rule. Prosecutors and police departments would be put on notice that they should not always be looking for loopholes to the warrant requirement. They would know that in the future, documents that do not satisfy the Fourth Amendment's warrant requirement more likely than not will not justify the search of a citizen's person, papers, and effects.

Giving law enforcement the benefit of the good faith exception in this case also conflicts with *Davis*. At the time the search was conducted, multiple judicial opinions interpreting § 2703(d) or state analogues required a warrant, and the statute itself instructed the government to get a warrant. The law was, at best, unsettled and in no respect could have been deemed to clearly authorize the government lawyer's choice to circumvent the ordinary warrant requirement.

The panel decided that law enforcement may rely on a *lack* of binding authority. Pet. App. 130a-131a. This turns *Davis* on its head. This Court has never used the good faith exception to allow the government to consider only those judicial decisions that interpret the Fourth Amendment more permissively and to ignore decisions with a stricter reading of law enforcement's constitutional obligations.

Moreover, the federal circuit courts of appeal and highest courts of several states have split over how to apply the good faith exception when a constitutional question remains open. In the majority of circuits, if the legal question remains ultimately unsettled, the exclusionary rule applies if the police conduct a search that is later deemed unconstitutional. As the Eleventh Circuit explained, police act objectively reasonably when relying on legal positions that are announced in a "bright line judicial rule," equating good faith to relying on appellate precedent that has already authoritatively determined the constitutionality of a particular search. *See United States v. Davis*, 598 F.3d 1259, 1267 (11th Cir. 2010), *aff'd* 564 U.S. 229 (2011). In contrast, when the legal issue is unresolved and "when law enforcement officers rely on precedent to resolve legal questions as to which reasonable minds

may differ[,] the exclusionary rule is well-tailored to hold them accountable for their mistakes." *Id.* (internal quotation omitted). *See also United States v. Curtis*, 635 F.3d 704, 714 n.27 (5th Cir. 2011) (holding that the good faith exception only applies if the answer to the constitutional question is "unequivocal"); *United States v. Buford*, 632 F.3d 264, 276 & n.9 (6th Cir. 2011) (also requiring the support for the government's position to be "unequivocal" before applying the good faith exception).

State courts have also repeatedly interpreted the exclusionary rule as a means of ensuring that law enforcement will not search first and ask questions later, but will act in conformity with explicit Fourth Amendment requirements. *See, e.g., State v. Dearborn*, 786 N.W.2d 97, 109 (Wisc. 2010) ("Under our holding today, the exclusionary rule is inappropriate only when the officer reasonably relies on clear and settled precedent." The exclusionary rule does apply, however, "in the vast majority of cases where neither this court nor the United States Supreme Court have spoken with specificity in a particular fact situation."). Indeed, Maryland's highest court, the very state with concurrent jurisdiction over the robberies at issue here, has held that when the answer to the constitutional question is unclear, the exclusionary rule applies. *Briscoe v.* State, 30 A.3d 879, 882-83 (Md. 2011) ("The principle that emerges from *Davis* is that operation of the exclusionary rule is suspended only when the evidence seized was the result of a search that, when conducted, was a 'police practice' specifically authorized by the jurisdiction's precedent in which the officer operates.").

In this case, however, although it acknowledged that the Fourth Amendment question was unresolved and had resulted in conflicting decisions from other courts, the Fourth Circuit granted law enforcement the discretion to hazard the more permissive side of an ongoing constitutional debate. When the issue is unsettled, the majority of courts "reject the government's invitation to allow police officers to rely on a diffuse notion of the weight of authority around the country." *United States v. Martin*, 712 F.3d 1080, 1082 (7th Cir. 2013). This Court should grant certiorari to resolve this open question and ensure that, when the law is unsettled, law enforcement must err on the side of following the Fourth Amendment's warrant requirement.

Conclusion

This case presents a recurring issue regarding the Fourth Amendment implications of the government's use of evolving technology to increase its ability to surveil Americans. This Court should grant the petition to provide needed guidance.

Respectfully submitted,

JAMES G. CONNELL, III
Connell Law, L.L.C.
P.O. Box 141
Cabin John, MD 20818
(703) 623-8410
jconnell@connell-law.com

JAMES WYDA
Federal Public Defender
District Of Maryland
MEGHAN SKELTON
Appellate Attorney
Counsel of Record
6411 Ivy Lane, 7th Floor
Greenbelt, Maryland 20770
(301) 344-0600
meghan_skelton@fd.org

Attorneys for Petitioner