No. 16-6308

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

Reply Brief for Petitioner

JAMES G. CONNELL, III
Connell Law, L.L.C.
P.O. Box 141
Cabin John, Maryland 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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

STATE & FEDERAL CASES

STATUTES

Reply Brief for Petitioner

In its effort to dissuade the Court from providing much-needed guidance on an issue of daily national importance, the government minimizes the fractured state of the law. It asks this Court to accept that what was good for rotary phones is good for data in the digital age. And it does so based upon the broadest possible reading of this Court's early third-party doctrine cases, *United States v. Miller,* 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), and the narrowest possible reading of more recent cases applying the Fourth Amendment to technologically enhanced searches or searches of digital information. *See Riley v. California*, 134 S. Ct. 2473 (2014); *Florida v. Jardines*, 133 S. Ct. 1409 (2013); *United States v. Jones*, 132 S. Ct. 945 (2012); *Kyllo v. United States,* 533 U.S. 27 (2001).

It may be that the government is correct and the third-party doctrine lives on, swallowing an individual's privacy interest in data that she generates so long as it is collected and held by a third-party service provider. Perhaps the government can use whatever sophisticated computational techniques it can devise to mine the increasingly detailed data that individuals unwittingly generate about themselves. But if this is so, and individuals do not have the right to exclude the government's prying eyes from their digital papers and effects—absent a warrant supported by probable cause—then this Court needs to inform magistrate judges, lower courts, and the public about their diminished privacy in the digital era.

I. The Court should grant the petition for certiorari to resolve continuing disagreements over important digital privacy issues.

In constitutionally significant ways, digital is different. Individuals passively

generate vast quantities of data about their location, activities, and associations as a result of the necessary use of cell phones to participate in 21st century society. The time has come for this Court to review the "dragnet type law enforcement practice[]" of monitoring an individual's location at all hours of the day and night over the course of months. *Cf. United States v. Knotts,* 460 U.S. 276, 283 (1983).

Do citizens voluntarily convey location data by using a cell phone? As they drive north on I-95 from Baltimore to Philadelphia, the answer changes. Relying on *Smith*, the Fourth Circuit held that people have no privacy interest in their location and movement over time so long as they can be reconstructed using historic cell site location information (CSLI). That is because, according to the Fourth Circuit, citizens voluntarily convey their location information to the equipment of cellular service providers. Pet. App. 12a. The Third Circuit came to 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 of U.S. for an Order Directing a Provider of Elec. Commc'n Service to Disclose Records to Gov't,* 620 F.3d 304, 317 (3d Cir. 2010) [hereinafter *In re Application (Third Circuit)*].

This split in reasoning is open and acknowledged. The Fourth Circuit recognized that its conclusion conflicted with that of the Third Circuit. Pet. App. 5a. As recently as late January 2017, lower federal courts continue to identify the split. *See United States v. Smith*, 2017 U.S. Dist. Lexis 11910 at *16-*17 (E.D. Pa. Jan. 26, 2017) (finding that it was bound by the Third Circuit's decision that individuals maintain a privacy interest in their location if conveyed to cellphone providers, although that decision conflicts with the rule in the Fourth, Fifth, Sixth, and

Eleventh Circuits).

Seeking to minimize this important divide, the government asserts that the Third Circuit's decision rested only on statutory construction rather than on constitutional grounds. (BIO 34.) In fact, although it also addressed the government's statutory construction arguments, the Third Circuit analyzed the types of privacy interests that the Fourth Amendment protects. It expressly considered (and rejected) the government's arguments regarding *Smith* and *Miller* and their constitutional holdings. *In re Application (Third Circuit)*, 620 F.3d at 317. When the Third Circuit rejected the government's argument that the government's use of CSLI implicates "no constitutional protections because the subscriber has shared its information with a third party, i.e., the communications provider," it resolved a Fourth Amendment question. *Id.* Its decision was not limited to how a magistrate judge should apply 18 U.S.C. § 2703(d), but rather addressed the scope of Fourth Amendment protection and whether the third-party doctrine eliminated the relevant privacy interest.

The government also states that the conflicting results and requests for guidance from United States magistrate judges do not merit review from this Court. While no individual decision of a magistrate judge on an application for a court order under 18 U.S.C. § 2703(d) may merit review, the conflicts among magistrate judges show the practical challenges faced by the judges forced to issue or deny orders without this Court's guidance. Moreover, the exponential growth of sealed law enforcement requests for access to historic CSLI underscores the importance of the

issue.[1]

II. This Court should grant certiorari to review an important and unresolved question about how to apply analogue precedents to technologically enhanced searches in the digital age.

The government's opposition rests on the premise that a technologically enhanced search or data search is not meaningfully different from a search of physical space or objects. This Court, however, has criticized that premise. "It would be foolish to contend that the degree of privacy secured by the Fourth Amendment has been entirely unaffected by the advance of technology." *Kyllo*, 533 U.S. at 33-34. In *Riley*, the Court rejected an "analogue test" to gauge Fourth Amendment privacy rights because such a test "would keep defendants and judges guessing for years to come." *Riley*, 134 S. Ct. at 2493. Instead, a technologically enhanced search, indeed a search like the one that took place here that would not be possible without the use of advanced computer technology, "must rest on its own bottom," rather than a "mechanical application" of decades-old exceptions and doctrines. *Id.* at 2489, 2484.

A. Metadata like CSLI is exactly the sort of private information the Fourth Amendment is intended to protect.

The government disputes the magnitude of the privacy intrusion that occurs when the government reconstructs a citizen's daily movements using historical CSLI. (BIO 27-28.) The government's opposition treats historic CSLI as if it is a simple piece of routing information for a single, discrete call. But the government

---

[1] *See* Amicus Brief of Electronic Frontier Foundation, *et al.*, at 12-14 (detailing the quantity of law enforcement requests for CSLI—more than 125,000 requests in 2015 just to AT&T and Sprint).

aggregated literally thousands of latitude and longitude coordinates from a seven-month period to retroactively retrace the petitioner's location and movements.

The government used the location of petitioner's phone to pinpoint the location of the petitioner himself for months at a time. In *Riley*, this Court relied on Justice Sotomayor's concurrence in *Jones* to describe the significance of the intrusion at issue here: "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; *see also id.* (describing location information over time as providing a comprehensive record of someone's movements "that reflect a wealth of detail about her familial, political, professional, religious, and sexual associations.") (quoting *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring)).

The government attempts to distinguish between content, which indisputably is protected by the Fourth Amendment, and what it claims is the virtually meaningless location data. (BIO 23.) Technology has eroded this once-important distinction in constitutionally significant ways.

The information at issue here is not confined to routing. It included the initiating and target phone numbers, the duration of the call, the time of the call, and the latitude and longitude of the cell towers that the phone had connected to at the beginning and end of the call. *(See* JA 2668-3102.) This information provides the government such specific insight into a person's beliefs, activities, associations, and plans that the government regularly uses it to plan drone strikes abroad. General Michael Hayden, former director of the CIA and NSA famously said, "We kill people

based on metadata."[2] Former NSA General Counsel Stewart Baker likewise said, "Metadata absolutely tells you everything about somebody's life. If you have enough metadata you don't really need content."[3]

When aggregated using sophisticated software, historic CSLI reveals a person's location at a church, union hall, AA meeting, or abortion clinic. *See Riley*, 134 S. Ct. at 2490. This private information is exactly what the Founders sought to protect when drafting the Fourth Amendment. The fact that the government acquires this information using a corporate records subpoena for information that it legally requires cellular phone providers to keep, instead of a warrant supported by probable cause, raises an important question of federal law that merits review by this Court.

B. The third-party doctrine, not protection for private information, is the historical aberration.

The government argues that the broader privacy concerns raised by its examination of CSLI do not justify a novel Fourth Amendment rule. (BIO 26.) No novel rule is necessary to protect papers and effects, digital or otherwise. The

---

[2]General Hayden made these comments at The Johns Hopkins Foreign Affairs Symposium, The Price of Privacy: Re-Evaluating the NSA (April 7, 2014), available to watch at https://www.youtube.com/watch?v=kV2HDM86XgI (last visited on February 21, 2017). This comment comes at 0:18:02. The metadata that General Hayden referred to reveals even less than what the government obtained here. The metadata justifying drone strikes included the time of the call, the originating number, target number, and the duration, but did not include location information. Imagine how much more telling that metadata would be with the location information that the government obtained here.

[3] https://www.wired.com/2015/03/data-and-goliath-nsa-metadata-spying-your-secrets/ (last visited on February 21, 2017).

third-party doctrine itself, which the government embraces, is arguably the novel rule the Framers would not recognize.[4] Moreover, the fact that such different approaches are found in *Smith* and *Miller*, as compared to *Riley, Jardines, Jones*, and *Kyllo* is in fact a reason to grant review—courts need to know which approach is the correct one to apply to digital and technologically enhanced searches.

For the first two hundred years of the Republic, this Court did not apply the "reasonable expectation of privacy" test derived from Justice Harlan's concurrence in *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring), extended into the third-party doctrine in *Miller* and *Smith*. More recently, however, this Court has returned to Fourth Amendment principles that predated *Katz*. *See generally Jardines*, 133 S. Ct. at 1414-16; *Jones*, 132 S. Ct. at 950-51; *Kyllo*, 533 U.S. at 34-36. In *Riley*, this Court warned that applying pre-digital principles could cause a significant diminution in privacy, below that level which the Founders anticipated protecting. *See* 134 S. Ct. at 2493; *see also Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (opining that the reasonable expectation of privacy test "is ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.").

Rather than producing a new rule, this case presents the Court with the opportunity to provide guidance on applying fundamental Fourth Amendment principles to digital information. Like the heat in *Kyllo* and the odors in *Jardines*, data that people unwittingly emit about their movements can be seized and

---

[4] *See* Amicus Br. of The Cato Institute at 1-2, 7-8; Amicus Curiae Br. of U.S. Justice Foundation, *et al*., at 10-19.

searched. *See United States v. Ackerman*, 831 F.3d 1292, 1307 (10th Cir. 2016) (seizing data, even where there is no physical trespass, appears to be a trespass to chattels in a way that courts during the founding era would have recognized).

For example, in *Jardines*, this Court resolved the case using founding-era trespass theory. Although the police entered private property seemingly based upon an implicit license to approach the front door, the Court decided that the police exceeded the scope of that license. By introducing a technologically enhanced search practice (a specially trained drug-sniffing canine), the government trespassed on a Fourth Amendment-protected property and privacy interest. 133 S. Ct. at 1416. The Court held that "the scope of the license—express or implied—is limited not only to a particular area but also to a particular purpose." *Id.* Thus, this Court's most recent discussion of the Fourth Amendment's role in a technologically enhanced search of information that is exposed to the public does not turn on the exposure. It turns on whether the government may use technology to exploit a limited and perhaps inadvertent exposure to reveal what otherwise is presumed private.

The government here argues that individual cell phone users cannot expect privacy, but rather assume the risk that the law enforcement will obtain their location information, because they know they convey radio frequency signals to the phone company. (BIO 19-20.) This argument is an eerie echo of the discredited and overruled majority opinion in *Olmstead v. United States*: "The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house, and message while passing over them, are not within the protection of the Fourth

Amendment." 277 U.S. 438, 466 (1928).

The government here relies on the same emission theory that controlled the outcome in *Olmstead*, but was overruled in *Katz*, *Kyllo*, and *Jardines*. No reasoned distinction exists between signals emitted from a phone that can be decoded to reveal conversation and radio signals emitted from cell phones that can be decoded to reveal location. *Kyllo* and *Jardines* make clear that the relevant issue is not the signal leaving the phone—or heat or odor emitting from a house—but the government's acquisition of individually meaningless datum and use of technology to transform the aggregated data to render the invisible visible.

Nevertheless, even if the third-party doctrine remains alive and well, this Court should grant review to clarify how *Smith* and *Miller* should apply in the digital age. The court below found that the very act of carrying a cell phone constituted a voluntary choice to convey personal location information. Pet App. 17a. This view fails to account for the fact that individuals generate highly detailed, private data regarding their movements over time, as encoded in CSLI, passively and automatically. *See Commonwealth v. Augustine*, 4 N.E.3d 846, 862 (Mass. 2014). CSLI is generated when citizens do nothing but carry a phone—missing a call creates CSLI. If this qualifies as conveying information at all, it is compulsory, not voluntary.

Moreover, a wide gulf separates the limited information discernible from a pen register and the comprehensive picture of a person's daily movements, interests and activities that CSLI allows the government observe. Even under *Miller*, the nature of the documents was critical to the Court's decision that individuals do not have a

privacy interest. The documents were "not confidential communications but negotiable instruments." *Miller*, 425 U.S. at 442. A person's movements over time as revealed by CSLI, on the other hand, are confidential.

C. Examining location by inspecting CSLI is a search.

The government claims that aggregating and processing this data was not a search, and thus not governmental action covered by the Fourth Amendment, because the government inferred where the petitioner was at any given point. (BIO 23.) The government relies on a footnote in *Kyllo* for the proposition that "an inference is not a search." *Kyllo*, 533 U.S. at 33 n.4. The complete quote undercuts the government's argument, however. After stating that the dissent was correct to say that the simple act of drawing an inference is not a search, the majority opinion continues, "That has no bearing, however, up on whether hi-tech measurement of emanations from a house is a search." *Id. Kyllo* further defined a search as "to examine by inspection." *Id.* at 33 n.1.

Thus, as *Kyllo* makes clear, using technology to make something that was imperceptible visible is a search. *Id.* at 34; *Jardines*, 133 S. Ct. at 1416. Here, petitioner's past movements were invisible. But the government compelled the cell phone service provider to deliver data generated by the petitioner's conduct, then generated a map plotting thousands of location points. This was not simply drawing an inference, but mapping a person's movements from otherwise invisible radio frequency signals. The government processed the data to decode a citizen's private movements.

D. Obtaining CSLI data with a corporate records subpoena is constitutionally unreasonable.

The government opposes further review on the grounds that the subpoena provision of the Stored Communications Act, 18 U.S.C. § 2703(d), is reasonable under the Fourth Amendment and reflects a valid weighing of privacy interests by Congress. (BIO 30-31.) The existence of the Stored Communications Act, part of a package of legislation enacted when cell phones were in their infancy and before historic CSLI was even a technological possibility, provides no bar to review. Congress could not have given meaningful consideration to the privacy implications of enacting 18 U.S.C. § 2703(d) because the type of data did not exist. Cell phones were not the pervasive appendages to human anatomy that they are today. *See Riley*, 134 S. Ct. at 2484. And the vast trove of data available for the government to mine at will did not exist. Thirty years ago, Congress could not have meaningfully considered historic CSLI either as a law enforcement tool or as a source of intensely private information.

Moreover, obtaining historical CSLI with a corporate records subpoena does not satisfy the Fourth Amendment's reasonableness requirement. Subpoenas, issued on a standard far lower than probable cause, protect the privacy interests of the person with the record, not the target of the search. The warrant requirement, on the other hand, protects the privacy interests of the person whose person, places and effects are subject to the search and seizure. In light of the object of the search—the data about a person's location—and the highly private nature of that information, the constitutionally protected interest is that of the individual, not the cellular service provider. In any event, if the interests are relatively equivalent, under the

Fourth Amendment's presumption that warrantless searches are unreasonable, the tie goes to the warrant requirement.

The government's claim that historic CSLI is a business record is correct only insofar as Sprint is a business and CSLI is recorded. But here, the object of the government's search was not a record of transactions between the petitioner and Sprint. The government made use of a tool, available only through technological advancements of the last few years, to observe the petitioner's past movements over time, as reflected in the data that he generated and Sprint happened to record. Citizens retain their rights to their confidential information, and do not transfer their interest in it to cellular service providers simply by making use of the service. *See United States v. Warshak*, 631 F.3d 266, 286-87 (6th Cir. 2011) (using a carrier's network does not transform confidential information about communications into jointly owned property).

III. This case presents an ideal vehicle to resolve the questions presented.

The government argues that the Court should deny the petition here because it recently denied review in two cases that presented similar issues,[5] and no reason exists to review this case in light of those denials. (BIO14.) However, in *Davis v. United States*, the government argued that the Fourth Amendment question did not warrant review because en banc consideration of *this* case was still pending.[6] The

---

[5] *See Davis v. United States*, 136 S. Ct. 479 (2015) (No. 15-146); *Guerrero v. United States*, 135 S. Ct. 1548 (2015) (No. 14-7103).

[6] Brief of the United States in Opposition at 12, *Davis v. United States*, 136 S. Ct. 479 (2015) (No. 15-146).

government implied that the Court should decline reviewing *Davis* while waiting for this case to mature.

The government posits two reasons why this case is not a good vehicle to resolve the questions presented: that any error is harmless and that the good faith exception to the exclusionary rule would apply, leaving the petitioner without meaningful relief. Neither is correct, and neither provides a reason to deny review.

The government's argument that the error is harmless (BIO 42) provides no impediment to review. For good reason, this Court's practice is to resolve the constitutional question, then allow the lower court to assess the effect of the erroneously admitted evidence. *See Lilly v. Virginia*, 527 U.S. 116, 139 (1999). The Fourth Circuit did not address harmless error. And this Court generally "decline[s] to address it in the first instance." *Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 329 n.14 (2009).

Nevertheless, the error was not harmless. The government used the CSLI at the earliest stages of its investigation into several unsolved robberies, which later became the basis for multiple new counts in a superseding indictment. Its improper use of CSLI therefore led to other evidence derived from the constitutional error, which is likely to be fruit of the poisonous tree. *See Wong Sun v. United States*, 371 U.S. 471, 488 (1963). The government repeatedly relied on the CSLI in its closing argument to the jury, specifically asking the jury to consider the CSLI in rendering its verdict. *See United States v. Jackson*, 636 F.3d 687, 697 (5th Cir. 2011) (opining that the government cannot "conclusively show" harmlessness when it relies on the erroneously admitted evidence in closing argument). The government cannot meet

its burden of proving that the error was harmless beyond a reasonable doubt. *See Fahy v. Connecticut*, 375 U.S. 85, 86-87 (1963).

Rather than being an impediment to review, the Fourth Circuit's treatment of the good faith exception is a reason to grant review. The government argues that because *Davis v. United States*, 564 U.S. 229 (2011), permits law enforcement to rely in good faith on binding authority to conduct a search, it is equally empowered to rely on a *lack of* binding authority. (BIO 42) As petitioner argued (Pet. 35-36, 39), *Davis* does not establish such a rule: binding authority and lack of binding authority are not equivalent. This Court has not addressed how the good faith exception applies when the law is unsettled.[7] *See id* at 250 (Sotomayor, J., concurring). In fact, the majority of lower courts hold that a lack of authority renders the good faith exception unavailable. *See* Pet. at 38-39. Thus, the Fourth Circuit's treatment of the good faith exception implicates another split, requiring this Court's guidance.

The government also asserts (BIO 39) that the exclusionary rule should not apply here because the government relied in good faith on a statute. *See Illinois v. Krull*, 480 U.S. 340, 350, 258 (1987). But law enforcement cannot rely in good faith on a statute after a court questions the statute's constitutionality. *Id.* at 352. As discussed above, multiple courts had already questioned that statute, something that the attorney who sought the court orders should have known.

---

[7] The government claims that the petitioner has not established that the law was unsettled at the time that the prosecutor obtained the court orders. The court below, however, correctly recognized that the law was unsettled at the time. Pet. App. 131a. *See also* Appellants' Fourth Circuit Opening Brief at pp. 47-50.

Accepting the government's invitation to avoid review here because 18 U.S.C. § 2703(d) provides a basis upon which to apply the good faith exception would mean that this Court will never review the constitutional question. The government will always invoke good faith when relying on a corporate records subpoena rather than a search warrant, which would leave the constitutional issue effectively unreviewable. This would give the government "*carte blanche* to violate constitutionally protected privacy rights, provided, of course, that a statute supposedly permits them to do so." *Warshak*, 631 F.3d at 282, n.13. Retroactively tracking citizens using CSLI has become a favorite tool of law enforcement, and cellular service providers are inundated with court orders seeking this data. The good faith exception should not be a "perpetual shield against the consequences of constitutional violations." *Id.*

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, Maryland 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