No. 15-146

IN THE

Supreme Court of the United States

QUARTAVIOUS DAVIS,

Petitioner,

—v.—

UNITED STATES OF AMERICA,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE ELEVENTH CIRCUIT

REPLY BRIEF FOR PETITIONER

Steven R. Shapiro
Nathan Freed Wessler
Jameel Jaffer
Ben Wizner
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
New York, NY 10004

Nancy Abudu
ACLU FOUNDATION OF FLORIDA, INC.
4500 Biscayne Boulevard, Suite 340
Miami, FL 33137

Benjamin James Stevenson
ACLU FOUNDATION OF FLORIDA, INC.
P.O. Box 12723
Pensacola, FL 32591-2723

David Oscar Markus
Counsel of Record
MARKUS/MOSS PLLC
40 N.W. 3rd Street, Penthouse One
Miami, FL 33128
(305) 379-6667
dmarkus@markuslaw.com

Jacqueline E. Shapiro
40 N.W. 3rd Street, Penthouse One
Miami, FL 33128

Attorneys for Petitioner

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

REPLY BRIEF FOR PETITIONER

When the Stored Communications Act ("SCA") was enacted in 1986, cell phones cost over $3,000 and were the size of a large brick. Less than one eighth of one percent of the U.S. population owned one. There were only 1,000 cell phone towers in the United States.[1] A lot has changed since then. Now, almost everyone carries a cell phone.

The government's position is that two cases from the 1970s, decided before the SCA was passed and even before cell towers were in use, permit law enforcement to obtain location information without a warrant. The government acknowledges, however, that the Fourth Circuit disagrees with its position and that there is a circuit conflict between the Eleventh and Fourth Circuits. In addition, this Court and numerous lower courts, including the Third Circuit and the Florida Supreme Court, have declined to extend old Fourth Amendment cases to "modern cell phones, which 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." *Riley v. California*, 134 S. Ct. 2473, 2484 (2014) (refusing to extend to cell phones the search-incident-to-arrest exception to the warrant requirement).

Recognizing the difficulty in applying these old cases to the entirely different world in which we now live, the government advocates that the Eleventh

---

[1] Andrea Meyer, *30th Anniversary of the First Commercial Cell Phone Call*, Verizon (Oct. 11, 2013), https://www.verizonwireless.com/news/article/2013/10/30th-anniversary-cell-phone.html.

Circuit's novel approach to the Fourth Amendment—allowing expansive warrantless search and seizures based on a standard well short of probable cause—be permitted to stand. The issues involved in this case are of national importance. They affect all of us, and they have been thoroughly aired in the lower courts. This Court's review is warranted.

1. As explained in the Petition and Supplemental Brief, the Eleventh Circuit is in conflict with the Third and Fourth Circuits on the central Fourth Amendment questions in this case. Pet. 24–28; Pet. Supp.1–5. The government acknowledges the conflict with the Fourth Circuit's opinion in *United States v. Graham*, 796 F.3d 332 (4th Cir. 2015). BIO 26–27. The filing of a petition for rehearing does not eliminate that conflict, nor does a court's request for a response to the rehearing petition. Unless and until the panel decision is vacated or reversed, the Fourth Circuit's panel opinion remains good law and the conflict persists.

Even if the Fourth Circuit were to grant rehearing en banc and reverse the panel opinion, the Eleventh Circuit's opinion would still conflict with the Third Circuit's decision in *In re Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 620 F.3d 304 (3d Cir. 2010) ["*Third Circuit CSLI Opinion*"]. That case assessed, *inter alia*, whether magistrate judges have the discretion to reject applications for historical CSLI submitted pursuant to 18 U.S.C. § 2703(d), and instead to insist on warrant applications.

Answering that question was not merely an exercise in statutory interpretation as the

government claims, BIO 27, but also involved application of the Fourth Amendment. 620 F.3d at 312–13, 317–19. The Third Circuit first engaged in statutory analysis, holding that under the plain language of § 2703, magistrate judges have discretion to reject applications for § 2703(d) disclosure orders if they determine that Fourth Amendment privacy interests necessitate the protections of a warrant. *Id.* at 315–17, 319. The court then went on to address the government's contention "that no CSLI can implicate constitutional protections because the subscriber has shared its information with a third party, i.e., the communications provider. For support, the Government cites *United States v. Miller*, 425 U.S. 435[] (1976), . . . [and] *Smith v. Maryland*, 442 U.S. 735[] (1979)." *Id.* at 317. Contrary to the Eleventh Circuit, the Third Circuit rejected this argument, noting that the third-party doctrine does not apply because "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way." *Id.* Other courts have subsequently cited the Third Circuit for this conclusion. *See, e.g.*, *Graham*, 796 F.3d at 355; *Tracey v. State*, 152 So. 3d 504, 522 (Fla. 2014); Pet. App. 78a.

The government also is too quick to distinguish the Florida Supreme Court's decision in *Tracey*. To be sure, that case involved warrantless government access to real-time cell site location information, and the court did not explicitly address Fourth Amendment protections for historical CSLI. 152 So. 3d at 515. However, the government attaches far more significance to that distinction than it deserves. *See* Pet. 23. Moreover, the location data at

issue in the two cases is identical. Just as here, in *Tracey* the government obtained "cell site location information," meaning information about which cell tower and directional sector of that tower the phone connected to "when a cell phone call occurs," rather than precise GPS coordinates or data obtained from the cell phone when not in active use. 152 So. 3d at 507 & n.1. The only difference in the data is that *Tracey* involved just one day of tracking, *id.* at 507, whereas this case involves 67 days of cell phone location data.

In any event, this case presents "an important question of federal law that has not been, but should be, settled by this Court." Rule 10(c). As explained in the Petition, the large volume of law enforcement requests for CSLI and the conflicting patchwork of legal standards governing access to it requires resolution by this Court. Pet. 14–22. In three separate opinions, six courts of appeals judges have explained their conclusion that there is a reasonable expectation of privacy in historical CSLI, and that the third-party doctrine does not apply. *Graham*, 796 F.3d at 338–61 (Davis, J., joined by Thacker, J.); Pet. App. 75a–101a (Martin, J., dissenting, joined by Jill Pryor, J.); Pet. App. 102a–122a (Sentelle, J., joined by Martin & Dubina, JJ.). Another four judges have explained that requests for historical CSLI raise substantial Fourth Amendment issues, without deciding whether the warrant requirement applies. *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 622–24 (5th Cir. 2013) (Dennis, J., dissenting) ["*Fifth Circuit CSLI Opinion*"]; *Third Circuit CSLI Opinion*, 620 F.3d at 312–13, 317–19 (Sloviter, J., joined by Roth, J.); *id.* at 320 (Tashima, J., concurring). In five opinions, ten courts of appeals

judges have concluded that there is no reasonable expectation of privacy in historical CSLI. *Graham*, 796 F.3d at 378–90 (Motz, J., dissenting in part); Pet. App. 13a–38a (Hull, J., joined by Ed Carnes, C.J., Tjoflat, Marcus, & Julie Carnes, JJ.); *id.* at 44a–49a (William Pryor, J., concurring); *id.* at 57a (Rosenbaum, J., concurring); *Fifth Circuit CSLI Opinion*, 724 F.3d at 608–15 (Clement, J., joined by Reavley, J.). This thorough vetting of the question presented provides this Court with a more-than-sufficient basis for review.

2. The government contends that *United States v. Miller* and *Smith v. Maryland* are controlling. For the reasons set forth in the Petition, these decisions are distinguishable, and do not dictate the outcome of this case. Pet. 31–33. Perhaps more importantly, the various opinions in *United States v. Jones*, 132 S. Ct. 945 (2012), and *Riley v. California*, 134 S. Ct. 2473 (2014), demonstrate a recognition that traditional Fourth Amendment principles may need to be reexamined in light of new digital realities. *See Riley*, 134 S. Ct. at 2489 ("A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom."); *Jones*, 132 S. Ct. at 958, 964 (Alito, J., concurring in the judgment) ("[I]t is almost impossible to think of late–18th-century situations that are analogous to what took place in this case. . . . [S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an

individual's car for a very long period."). These principles include the third-party doctrine and the question of what constitutes a reasonable expectation of privacy in an increasingly digital world. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

The government's "mechanical application," *Riley*, 134 S. Ct. at 2484, of *Miller* and *Smith* would subject to warrantless search "a staggering amount of information that surely must be protected under the Fourth Amendment," from emails and cloud-stored documents, to comprehensive internet browsing and search histories, and much, much more. Pet. App. 81a–84a. This Court should take the opportunity to clarify the reach of precedents now nearly four decades old to the voluminous and exceedingly sensitive digital records that twenty-first-century Americans cannot avoid creating as they go about their daily lives.

3. The government understates the privacy implications of the disclosure order in this case by stating that "the historical cell-site records obtained in this case revealed only that petitioner . . . was in the general vicinity of six robberies around the time that those robberies occurred." BIO 22. The government itself characterized those records very differently at trial, arguing to the jury that the records placed Petitioner's phone "literally right up against" and "literally right on top of" specific locations at specific times. Pet. 10 (citing trial transcript). While the government's trial strategy

expressly relied on the accuracy of 39 of Petitioner's location data points that it believed corroborated its theory of the case, *see* Gov't Ex. 37A–F, it defies logic to suggest the remaining 11,567 location points contained in Petitioner's CSLI records reveal nothing private about his life. Indeed, those records reveal "much information about Mr. Davis's day-to-day life that most of us would consider quintessentially private," including patterns of movement, whether he slept at home or elsewhere, and a great deal more. Pet. App. 92a; *see also Graham*, 796 F.3d at 348 ("Much like long-term GPS monitoring, long-term location information disclosed in cell phone records can reveal both a comprehensive view and specific details of the individual's daily life."); Electronic Frontier Foundation, et al., Amici Br. 10–15. Longer-term data about Petitioner's locations and movements reveals information that society recognizes as justifiably private, and warrantless acquisition of this information violates the Fourth Amendment.

Nor is the privacy violation mitigated because conclusions about an individual's exact location or activity based on CSLI records will sometimes rest on inferences. *See* BIO 16–17. As this Court has explained, "the novel proposition that inference insulates a search is blatantly contrary to *United States v. Karo*, 468 U.S. 705[] (1984), where the police 'inferred' from the activation of a beeper that a certain can of ether was in the home." *Kyllo v. United States*, 533 U.S. 27, 36 (2001). The introduction of an inferential step to interpret that otherwise protected information does not absolve the government from complying with the warrant requirement.

In recognition of the serious privacy concerns at stake, the State of California recently became the latest to require a warrant for law enforcement access to historical CSLI. Electronic Communications Privacy Act, 2015 Cal. Legis. Serv. Ch. 651 (to be codified at Cal. Penal Code § 1546.1(b)). Other states have enacted the same protection in the last several years. Pet. 23–24. These states' recognition of the expectation of privacy in CSLI supports application of the warrant requirement here.

4. The government attempts to defend the Eleventh Circuit's alternative (and novel) holding that the warrantless search and seizure of location information is reasonable under the Fourth Amendment by analogizing the SCA procedure to subpoenas of business records and papers. BIO 23–25. This analogy, however, proves too much. It would allow the government to acquire a breathtaking amount of data about a person, including the books one orders on Amazon, the apps one purchases, the newspapers and articles one chooses to download, the pictures one stores in the cloud, the music one purchases, and so on. All of this information is available from subpoenaing a third party connected to one's cell phone. Under the government's analogy, it will not only be able to "reconstruct someone's specific movements down to the minute," *Riley*, 134 S. Ct. at 2490 (citing *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring)), it will be able to reconstruct what that person is reading, playing, or listening to at that specific place.

For the same reason, the government's argument that individuals have a "diminished expectation of privacy in those records" must

fail. Otherwise, we will be forced to choose between using our cell phones as normal members of society and retaining our privacy. The government's appeal to its interest in stopping crime, BIO 25–26, is of course present in all cases, and it is precisely that interest that requires application of the warrant requirement. *Ferguson v. City of Charleston*, 532 U.S. 67, 81 (2001) (warrantless search is unreasonable where the purpose of the search "is ultimately indistinguishable from the general interest in crime control."); *see also Arizona v. Hicks*, 480 U.S. 321, 328 (1987) (explaining that the Court would not "send police and judges into a new thicket of Fourth Amendment law" where a search did not require probable cause). The government does not contend that this case falls under any specific exception to the warrant requirement, like the special-needs cases. Pet. 35.

The claim that intrusion on a reasonable expectation of privacy is reasonable without a warrant is a novel and dangerous approach to the Fourth Amendment, and one that should be reviewed and rejected by this Court. *Jones v. United States*, 357 U.S. 493, 499 (1958) (exceptions to the warrant requirement are to be "jealously and carefully drawn").

5. The government's reliance on the good-faith exception as a reason to deny review in this case is misplaced. There are strong reasons not to expand the good-faith exception to prosecutors. Unlike the statute at issue in *Illinois v. Krull*, 480 U.S. 340 (1987), the statute here gave prosecutors the option of obtaining a warrant supported by probable cause. 18 U.S.C. § 2703(c)(1)(a). And, unlike

police on the street, prosecutors are not making split-second judgments when deciding whether a warrant is needed. Prosecutors who choose not to seek a warrant assume the risk of suppression that flows from that decision. No decision of this Court has ever expanded the exception to a prosecutor or any other law enforcement officer under such circumstances. The government does not claim to the contrary. BIO 33.

Even if applicable, however, invocation of the good-faith exception is not a reason to deny the petition in this case. Otherwise, the government's decision to obtain historical CSLI without seeking a warrant in cases like this one will be effectively insulated from appellate review. *Compare Davis v. United States*, 131 S. Ct. 2419, 2433 (2011) ("[T]he good-faith exception in this context will not prevent judicial reconsideration of prior Fourth Amendment precedents."). Given the policies of cellular service providers, the government will *always* invoke the good-faith exception because it will never be able to obtain CSLI without adhering to the court-order provision of 18 U.S.C. § 2703(d) or demonstrating an emergency that precludes such process, *see id.* § 2702(c)(4). *See, e.g.*, AT&T, *Transparency Report* 8 (2015)[2] ("We require a court order signed by a judge for the production of historical cell site location information."); Sprint, *Sprint Corporation Transparency Report* 2 (July 2015)[3]; T-Mobile,

[2] http://about.att.com/content/dam/csr/Transparency%20Reports/Transparency/ATT_Transparency%20Report_July%202015.pdf.

[3] http://goodworks.sprint.com/content/1022/files/TransaparencyReportJuly2015.pdf.

Transparency Report for 2013 and 2014, at 2 (2015)[4] (requiring "Court Order or Warrant" for historical CSLI); Verizon, *Verizon's Transparency Report for the First Half of 2015*[5] ("Verizon only produces location information in response to a warrant or order; we do not produce location information in response to a subpoena."). If application of the good-faith exception were to insulate Fourth Amendment violations from review, "the government would be given *carte blanche* to violate constitutionally protected privacy rights, provided, of course, that a statute [or court order] supposedly permits them to do so. The doctrine of good-faith reliance should not be a perpetual shield against the consequences of constitutional violations." *United States v. Warshak*, 631 F.3d 266, 282 n.13 (6th Cir. 2010).

Respectfully Submitted,

David Oscar Markus
Counsel of Record
MARKUS/MOSS PLLC
40 N.W. 3rd Street,
Penthouse One
Miami, FL 33128
(305) 379-6667
dmarkus@markuslaw.com

[4] http://newsroom.t-mobile.com/content/1020/files/NewTransparency Report.pdf.

[5] http://transparency.verizon.com/themes/site_themes/transparency/ Verizon-Transparency-Report-US.pdf.

Jacqueline E. Shapiro
40 N.W. 3rd Street,
Penthouse One
Miami, FL 33128

Steven R. Shapiro
Nathan Freed Wessler
Jameel Jaffer
Ben Wizner
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street
New York, NY 10004

Nancy Abudu
ACLU FOUNDATION OF
FLORIDA, INC.
4500 Biscayne Blvd.,
Ste. 340
Miami, FL 33137

Benjamin James Stevenson
ACLU FOUNDATION OF
FLORIDA, INC.
P.O. Box 12723
Pensacola, FL 32591-2723

Dated: October 19, 2015