No. 16-402

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

—v.—

UNITED STATES OF AMERICA,

Respondent.

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

REPLY TO BRIEF IN OPPOSITION

Harold Gurewitz
GUREWITZ & RABEN, PLC
333 W. Fort Street, Suite 1400
Detroit, MI 48226

Daniel S. Korobkin
Michael J. Steinberg
Kary L. Moss
AMERICAN CIVIL LIBERTIES UNION FUND OF MICHIGAN
2966 Woodward Ave.
Detroit, MI 48201

Nathan Freed Wessler
Counsel of Record
Ben Wizner
Brett Max Kaufman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

David D. Cole
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
915 15th Street, NW
Washington, D.C. 20005

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

CONSTITUTION & STATUTES

RULES

OTHER AUTHORITIES

REPLY TO BRIEF IN OPPOSITION

When the Stored Communications Act ("SCA") was enacted in 1986, cell phones cost over $3,000, were the size of a large brick, could connect to only fragmentary cellular networks, and were used by very few people. Pet. 33. [1] Now, 95 percent of Americans own a cell phone, [2] and cellular tower coverage spans from coast to coast.

The government's position is that two cases from the 1970s, decided before the SCA was passed and before cell phones were available, permit law enforcement to obtain unlimited cell site location information ("CSLI") without a warrant. The government minimizes the split with the Third Circuit and downplays the importance of the issues at stake. Yet, this Court and lower courts have recognized that Fourth Amendment cases from a prior era cannot be applied mechanically 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).

The government urges that the Sixth Circuit's approach to the Fourth Amendment—allowing

---

[1] *See also* Verizon, *Celebrating 30th Anniversary of First Commercial Cell Phone Call* (Oct. 11, 2013), https://www.verizon.com/about/news/celebrating-30th-anniversary-first-commercial-cell-phone-call.

[2] Pew Research Center, *Mobile Fact Sheet* (2017), http://www.pewinternet.org/fact-sheet/mobile/.

expansive warrantless searches 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, the Sixth Circuit is in conflict with the Third Circuit on the central Fourth Amendment questions in this case. Pet. 22–23. The Third Circuit's opinion 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*"], 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 interpretation and 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. In direct contrast to the Sixth Circuit in the decision below, the Third Circuit rejected the government's 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 Tracey v. State*, 152 So. 3d 504, 522 (Fla. 2014); *In re Application for Telephone Info. Needed for Criminal Investigation*, 119 F. Supp. 3d 1011, 1029 (N.D. Cal. 2015).

This case also 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 require resolution by this Court. Pet. 12–24. Courts of appeals have exhaustively debated the issues at stake. In four separate opinions, eight 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. *United States v. Graham*, 824 F.3d 421, 441 (4th Cir. 2016) (en banc) (Wynn, J., dissenting in part and concurring in the judgment, joined by Floyd & Thacker, JJ.); *United States v. Graham*, 796 F.3d 332, 338 (4th Cir. 2015) (Davis, J., joined by Thacker, J.), *rev'd en banc,* 824 F.3d 421; *United States v. Davis*, 785 F.3d 498, 500 (11th Cir. 2015) (en banc) (Martin, J., dissenting, joined by Jill

Pryor, J.); *United States v. Davis*, 754 F.3d 1205, 1208 (11th Cir. 2014) (Sentelle, J., joined by Martin & Dubina, JJ.), *rev'd en banc*, 785 F.3d 498. Another five judges have explained that requests for historical CSLI raise substantial Fourth Amendment issues, without deciding whether the warrant requirement applies. Pet. App. 24a (Stranch, J., concurring); *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 615 (5th Cir. 2013) (Dennis, J., dissenting) ["*Fifth Circuit CSLI Opinion*"]; *Third Circuit CSLI Opinion*, 620 F.3d at 305 (Sloviter, J., joined by Roth, J.); *id.* at 319 (Tashima, J., concurring). In six opinions, 23 courts of appeals judges have concluded that there is no reasonable expectation of privacy in historical CSLI, with many of those explaining that they felt they lacked authority to part company with this Court's third-party doctrine precedents. Pet. App. 1a (Kethledge, J., joined by Guy, J.); *Graham*, 824 F.3d at 424 (Motz, J., joined by Traxler, C.J., Wilkinson, Niemeyer, King, Gregory, Shedd, Duncan, Agee, Keenan, Diaz & Harris, JJ.); *Graham*, 796 F.3d at 378 (Motz, J., dissenting in part); *Davis*, 785 F.3d at 500 (Hull, J., joined by Ed Carnes, C.J., Tjoflat, Marcus, & Julie Carnes, JJ.); *id.* at 519 (William Pryor, J., concurring); *Fifth Circuit CSLI Opinion*, 724 F.3d at 602 (Clement, J., joined by Reavley, J.). Other judges have concurred in this outcome but have written separately to raise concerns about the implications of applying this Court's third-party–doctrine cases to such sensitive data. *See Davis*, 785 F.3d at 521 (Jordan, J., concurring, joined by Wilson, J.); *id.* at 524 (Rosenbaum, J., concurring). This thorough vetting of the question presented coupled with the conflict between the Third and Sixth

Circuits 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 analog-era decisions do not dictate the outcome of this digital-era case. Pet. 28–32. As the various opinions in *United States v. Jones*, 565 U.S. 400 (2012), and *Riley v. California*, 134 S. Ct. 2473 (2014), demonstrate, "any extension of th[e] reasoning [from older Fourth Amendment cases] to digital data has to rest on its own bottom." *Riley*, 134 S. Ct. at 2489; *see also Jones*, 565 U.S. at 420, 430 (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."). Among the principles that require reexamination are the third-party doctrine and the question of what constitutes a reasonable expectation of privacy in an increasingly digital world. *Jones*, 565 U.S. at 417 (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* "appears to admit to no limitation on the quantity of records or the length of time for which such records may be compelled." Pet. App 29a. The government's

position therefore would subject to warrantless search "a staggering amount of information that surely must be protected under the Fourth Amendment," from personal emails and cloud-stored documents, to detailed and intimate internet browsing and search histories. *Davis*, 785 F.3d at 535 (Martin, J., dissenting). This Court should clarify the reach of precedents now 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 when it says that sensitive location information can only be "approximately inferred" from the CSLI records. BIO 22. The government itself characterized those records very differently at trial, arguing to the jury that the records placed Petitioner's phone "right where the first robbery was at the exact time of the robbery, the exact sector" and that he was "right in the right sector before the Radio Shack in Highland Park." Pet. 8 (citing trial transcript). Given that the government's trial strategy expressly relied on the accuracy of at least 16 of Petitioner's location data points that it believed corroborated its theory of the case, *see* Pet. App. 74a–89a, it cannot now credibly suggest that the remaining thousands of location points covering months of phone calls reveal nothing private about Petitioner's life. Those records reveal "much information about [a person's] day-to-day life that most of us would consider quintessentially private," including patterns of movement, whether she slept at home or elsewhere, and more. *Davis*, 785 F.3d at 540 (Martin, J., dissenting); *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. ["EFF Br."] 15–17. 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.

It is not dispositive that some cell site data is less precise than the GPS data at issue in *Jones*. *See* BIO 21. The size of cell site sectors varies widely. Some CSLI data points will locate a person relatively precisely, and others more approximately. EFF Br. 10–11. There is no way for an officer to know in advance whether a suspect's CSLI will reveal more or less precise location information, thus necessitating the protection of a warrant. *Cf. Kyllo v. United States*, 533 U.S. 27, 39 (2001). Moreover, as Judge Stranch explained, "precision is not the only variable with legal significance": duration and comprehensiveness of the surveillance also matter. Pet. App. 27a. The *four months* of location data collected here "far exceeds the threshold" of longer-term tracking identified in previous cases. Pet. App. 29a. And as *amici* explain, the precision and volume of CSLI data is constantly increasing, rendering all the more pressing the need for this Court to weigh in. EFF Br. 10–11.

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 18–19. 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*, 533 U.S. at 36. The introduction of an inferential step to reveal otherwise-protected information does not reduce the intrusion on privacy nor absolve the government from complying with the warrant requirement.

Indeed, in recognition of the serious privacy concerns at stake, a number of states require a warrant for law enforcement access to historical CSLI. Pet. 23 (citing state statutes); *see also* Cal. Penal Code § 1546.1(b); 12 R.I. Gen. Laws § 12-32-2. These states' recognition of the expectation of privacy in CSLI supports application of the warrant requirement here. Far from suggesting that the Court should defer to legislative judgements on the constitutional question before it, *see* BIO 24; Pet. App. 16a–17a, these legislative enactments evidence the growing societal understanding that cell phone location records should be shielded from warrantless search. That understanding further supports the conclusion that there is a reasonable expectation of privacy in CSLI.

4. The government argues that even if there is a privacy interest in CSLI, the warrantless search and seizure of the data is reasonable under the Fourth Amendment. BIO 22–26. But its analogy to subpoenas of business records and papers proves too much. The government's position would allow it to warrantlessly acquire a breathtaking amount of data about a person merely by subpoenaing a third

party connected to one's cell phone. That data includes not just the location information at issue in this case, but the books one orders on Amazon, the medical data one shares with a third-party health application, the political websites one visits, the smartphone applications one downloads, the newspapers and articles one chooses to read, the pictures one stores in the cloud, the music one purchases, even the heart-rate data gathered by a smartwatch and uploaded to the cloud. Under the government's view, an individual's use of a cell phone will enable the government to not only "reconstruct someone's specific movements down to the minute" without a warrant, *Riley*, 134 S. Ct. at 2490, but to reconstruct what that person was reading, playing, listening to, or doing 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. BIO 25. Otherwise, we will be forced to choose between using our cell phones as normal members of society and retaining our privacy. The government's interest in stopping crime, BIO 25–26, is present in all cases; far from diminishing the privacy expectation, it is precisely that interest that creates the risk of police overreaching and requires application of the warrant requirement as a bulwark of privacy. *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, nor could it, that this case falls under any specific exception to the warrant requirement such as exigency or "special needs."

The claim that such a far-reaching intrusion on a reasonable expectation of privacy is reasonable without a warrant is a novel and dangerous approach to the Fourth Amendment, and should be 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. Because the court of appeals did not rule on whether the good-faith exception to the exclusionary rule applies,[3] this case is a clean vehicle for this Court to consider the question presented. The absence of a good-faith ruling distinguishes this case from *Davis*, in which the Court denied certiorari last term. *See Davis*, 785 F.3d at 518 n.20, *cert. denied*, 136 S. Ct. 479 (2015). In this case, application of the good-faith exception should be decided in the first instance by the court of appeals on remand.[4]

In any event, 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

---

[3] The district court also did not provide a reasoned ruling addressing the good-faith exception, invoking the doctrine only in a single cursory footnote. Pet. App. 38a n.1.

[4] The court of appeals likewise did not reach decision on the government's argument that admission of the CSLI evidence was harmless error. That issue, too, should be addressed on remand.

probable cause. 18 U.S.C. § 2703(c)(1)(a). And, unlike police on the street, prosecutors, as officers of the court, are expected to scrupulously assess the Fourth Amendment interests at stake. *Cf. United States v. Leon*, 468 U.S. 897, 921 (1984). Prosecutors who choose not to seek a warrant where such a route is fully available assume the risk of suppression that flows from that decision. No decision of this Court has ever expanded the exception to a prosecutor under such circumstances.

Even if applicable, however, invocation of the good-faith exception is not a reason to deny the petition. Otherwise, the government's decision to obtain historical CSLI without seeking a warrant will be effectively insulated from appellate review. *Compare Davis v. United States*, 564 U.S. 229, 247 (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* 7 (2016) [5] ("[For historical location information] we require a General Court Order, search warrant, or probable cause court order, depending on the applicable state and federal laws."); *accord* Sprint, *Sprint Corporation Transparency*

[5] http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_TransparencyReport_July2016.pdf.

Report 2 (July 2016)[6]; T-Mobile, *Transparency Report for 2015*, at 2 (2016) [7] ; Verizon, *Verizon's Transparency Report 2H 2016*[8]. 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,

Nathan Freed Wessler
Counsel of Record
Ben Wizner
Brett Max Kaufman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

---

[6] http://goodworks.sprint.com/content/1022/files/Transaparency%20Report%20July2016.pdf.

[7] https://newsroom.t-mobile.com/content/1020/files/2015Transparency Report.pdf.

[8] https://www.verizon.com/about/portal/transparency-report/wp-content/uploads/2017/01/Transparency-Report-US-2H-2016.pdf.

David D. Cole
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
915 15th Street, NW
Washington, D.C. 20005

Harold Gurewitz
GUREWITZ & RABEN, PLC
333 W. Fort Street,
Suite 1400
Detroit, MI 48226

Daniel S. Korobkin
Michael J. Steinberg
Kary L. Moss
AMERICAN CIVIL LIBERTIES
UNION FUND OF
MICHIGAN
2966 Woodward Ave.
Detroit, MI 48201

Dated: February 10, 2017