No. 16-402

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

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

BRIEF OF *AMICUS CURIAE* THE RUTHERFORD INSTITUTE IN SUPPORT OF PETITIONER

JOHN W. WHITEHEAD
DOUGLAS R. MCKUSICK
THE RUTHERFORD INSTITUTE
P.O. Box 7482
Charlottesville, VA 22906
(434) 978-3888

D. ALICIA HICKOK
Counsel of Record
MARK D. TATICCHI
DRINKER BIDDLE & REATH LLP
One Logan Square
Philadelphia, PA 19103
(215) 988-2700
Alicia.Hickok@dbr.com

Counsel for Amicus Curiae

August 14, 2017

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D. C. 20002

QUESTION PRESENTED

Whether the warrantless seizure and search of historical cell phone records revealing the location and movements of a cell phone user over the course of 127 days is permitted by the Fourth Amendment.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

INTEREST OF *AMICUS CURIAE*[1]

The Rutherford Institute is an international non-profit civil liberties organization headquartered in Charlottesville, Virginia. Founded in 1982 by its President, John W. Whitehead, the Institute provides *pro bono* legal representation to individuals whose civil liberties are threatened and educates the public about constitutional and human rights issues.

As part of its mission, The Rutherford Institute resists the erosion of fundamental civil liberties that many would ignore in a desire to enhance the ability of governmental authorities to detect, deter, and prosecute criminal activity. The Rutherford Institute believes that according ever increasing power and authority to law enforcement only creates a false sense of security while sanctioning unnecessary intrusions upon the private lives of private citizens.

The Rutherford Institute is interested in this case because it is committed to ensuring the continued vitality of the Fourth Amendment. Affirming the judgment of the Court of Appeals would undercut the Amendment's protections by enabling long-term surveillance of individuals—and the concomitant invasion of privacy that such surveillance entails—without first obtaining a warrant from a neutral magistrate.

---

[1] All parties to this matter have granted blanket consent for *amicus curiae* briefs in support of either or neither party. Petitioner filed such consent on July 11, 2017, and Respondent filed such consent on July 26, 2017. The requirements of Rule 37.2(a) of the rules of this Court are satisfied by these filings. No counsel for a party authored this brief in whole or in part, and no party or counsel for a party made a monetary contribution intended to fund the preparation or submission of this brief. No one other than *amicus curiae*, its members, or its counsel made a monetary contribution to the preparation or submission of this brief.

INTRODUCTION AND SUMMARY OF ARGUMENT

In addressing petitioner's Fourth Amendment challenge, the Court of Appeals framed the correct question: Did petitioner have a reasonable expectation of privacy in the 127 days' worth of cell-site location information the government obtained from his wireless carrier? See *United States* v. *Carpenter*, 819 F.3d 880, 886 (6th Cir. 2016).

The court went astray, however, in failing to properly contextualize that inquiry. *First*, it erred by failing to ask whether today, in the here and now, society would be prepared to accept petitioner's privacy expectations as reasonable.

Second, it failed to take account of the nature of the government's request—a demand for four months' worth of petitioner's movements—a factor which the text and structure of 18 U.S.C. § 2703 clearly contemplates being taken into account.

In light of these errors, the Sixth Circuit's judgment must be reversed.

ARGUMENT

I. THE COURT OF APPEALS FAILED TO ASSESS CONTEMPORARY EXPECTATIONS OF PRIVACY IN ITS FOURTH AMENDMENT ANALYSIS.

The Court of Appeals' decision in this case is the product of a flawed analytical framework. Rather than test petitioner's Fourth Amendment claim by assessing the present-day social and cultural expectations regarding the privacy of individuals' movements in public, the Sixth Circuit analogized the facts of this case to those of disparate decisions—often decades

old—that arose in a much different factual, social, legal, and technological context than that which prevails today. See *Carpenter*, 819 F.3d at 887-889 (citing, *inter alia*, *Smith* v. *Maryland*, 442 U.S. 735 (1979), and *United States* v. *Miller*, 425 U.S. 435, 443 (1976)). That was error.

Instead, the Court of Appeals should have straightforwardly applied the test that this Court's cases command: Did Timothy Carpenter possess a reasonable expectation that his (approximate) location and (general) movements would remain free from governmental oversight? Cf. *United States* v. *Jones*, 565 U.S. 400, 430 (2012) (Alito, J., concurring in the judgment) ("The best that we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated.").

If the Court of Appeals had not focused its analysis *exclusively* on the facts of prior cases and had instead also assessed *current* social understandings, it would have answered that query in the affirmative and held that a request for cell-site location data must, in the typical case, be supported by a warrant issued by a neutral magistrate upon a finding of probable cause.

The discussion that follows canvasses some of the contextual factors not considered by the Court of Appeals and explains why they compel the conclusion that petitioner's rights were traversed by the government's warrantless procurement of his cell-site location information.

1. The Court of Appeals erred by ignoring the significance of *present-day* social expectations in the Fourth Amendment analysis. As several Members of

this Court recognized only a few Terms ago, time and technology change the public's perception of what is—and should be—safe from prying governmental eyes. *See Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) (invoking the "evolution of societal privacy expectations" in light of "technological advances"); *id.* at 427 (Alito, J., concurring in the judgment) ("Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes.").

In his concurrence in the judgment in *Jones*, Justice Alito posited one way in which technological change can shift that balance, suggesting that "[n]ew technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile." *Id.* at 427. People wishing to fly in an airplane, for example, agree to endure magnetometers, pat-down searches, and x-ray inspection of their luggage.

But the interaction between technology and expectations of privacy can also be less linear than the zero-sum tradeoff illustrated above might suggest. For example, technology can influence social understandings of how—and how broadly—an individual's information will be distributed when shared with a third party.

2. Social media provides a useful illustration. Take Facebook. The website's privacy guide assures users: "You have control over who sees what you share on Facebook." Facebook, Privacy Basics, https://www.facebook.com/about/basics/usr1 (last visited Aug. 7, 2017); Facebook, Privacy Basics: Likes & Comments, https://www.facebook.com/about/basics/manage-your-privacy/my-likes-and-comments#2 (last visited Aug. 7, 2017) ("The person who posts something has

control over the audience who can see it."). Thus, a Facebook user can publish information to a pre-populated list of recipients (*e.g.*, all individuals that the user has designated as "Close Friends") or create a customized list of recipients. Facebook, Privacy Basics: Posts, https://www.facebook.com/about/basics/manage-your-privacy/posts#11 (last visited Aug. 7, 2017); see also Facebook, Privacy Basics: Friend List, https://www.facebook.com/about/basics/manage-your-privacy/friend-list#1 (last visited Aug. 7, 2017) (informing users that they can restrict who may view a list of their Facebook contacts (*i.e.*, "friends")).

The website also allows users to see what their individual profile and pages look like—either to a class of other Facebook members (*e.g.*, members that are not designated as a "Friend" of the user) or to an individual Facebook member. Facebook, Privacy Basics: Profile, https://www.facebook.com/about/basics/manage-your-privacy/profile#6 (last visited Aug. 7, 2017). If the user learns that a third party can see information the user doesn't want that third party to see, that information can be restricted or deleted. Facebook, Privacy Basics: Profile, https://www.facebook.com/about/basics/manage-your-privacy/profile #10 (last visited Aug. 7, 2017). Similarly, if a Facebook user "post[s] something and later decide[s] [he or she] do[es]n't want people to see it, [the user] can delete it." Facebook, Privacy Basics: Deleting Posts, https://www.facebook.com/about/basics/manage-your-privacy/deleting-posts (last visited Aug. 7, 2017).

Indeed, users even have the ability to control who can see information about them that is posted by a *different* Facebook user. Facebook, Privacy Basics: Profile, https://www.facebook.com/about/basics/manage-your-privacy/profile#12 (last visited Aug. 7, 2017).

And that's just one social media site. Others afford users a similar degree of control over the information they share. See, *e.g.*, Google, Google+ Help: Use Circles on Google+, https://support.google.com/plus/answer/6320407?hl=en&ref_topic=6320382 (last visited Aug. 7, 2017) (explaining that users can add other Google+ members to a "circle"—*i.e.*, a collection of individuals who share something in common (being members of the user's family, fellow alumnae of her university, etc.)—and then choose which circle(s) will see each piece of information the user posts on Google+); Instagram, How Do I Set My Photos and Videos to Private So That Only Approved Followers Can See Them?, https://help.instagram.com/448523408565555 (last visited Aug. 7, 2017) (explaining that users can restrict access to a list of "followers" (*i.e.*, other Instagram members) whom the user must affirmatively approve before they can see information the user has posted to the social media site); LinkedIn, LinkedIn Help: Visibility of Your Updates, Posts, and Recent Activity, https://www.linkedin.com/help/linkedin/answer/61030 (last visited Aug. 7, 2017) (explaining that "[w]hen you share a post on your LinkedIn feed, you can choose whether to share your post publicly or to your connections only").

It is clear, moreover, that these media touch and affect an overwhelming number of the "people" with whom the Fourth Amendment is concerned. As of Q2 2017, Facebook alone boasted an average monthly user base of 236 million people in the U.S. and Canada. Facebook, Inc., Quarterly Report (Form 10-Q) at 22 (July 27, 2017), *available at* http://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/dffb94d1-5a1b-4ec2-8eb7-56901be40efd.pdf. In other words, even subtracting out one Facebook account for each of the

36.3 million residents of Canada,[2] that still leaves approximately 200 million accounts for the United States—nearly 65 percent of the country's population as of the last decennial census.[3]

3. In a similar vein, mobile phones and their applications ("apps") also offer users fine-grained control over dissemination of the users' information—and, in particular, the users' location information. Specifically, a user can decide which of the apps on his or her phone (if any) will be able to ascertain the phone's—and hence the user's—geographic location. See, *e.g.*, Apple, Inc., About Privacy and Location Services in iOS 8 and Later, https://support.apple.com/en-us/HT203033 (last visited Aug. 11, 2017) ("You can individually control which apps and system services have access to Location Services data.").

This allows users to exercise fully customizable control over the disclosure of their location information. So, for example, they may opt to allow the phone's ride-sharing (*e.g.*, Uber), navigation (*e.g.*, Google Maps), or weather apps to know where the user is located, but deny that information to social networking apps like Facebook or Instagram.

4. These contemporary expectations of nuanced control over the degree to which one's information will

---

[2] Government of Canada, *Statistics Canada*, Sept. 28, 2016, http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/demo02a-eng.htm (last visited Aug. 9, 2017).

[3] U.S. Census Bureau, *Population Distribution and Change: 2000 to 2010*, Mar. 2011, at 1, *available at* https://www.census.gov/prod/cen2010/briefs/c2010br-01.pdf (last visited Aug. 9, 2017). Were that not enough, Facebook also reports that, on each day during Q2 2017, an average of 183 million users logged onto its site. Facebook, Inc., Quarterly Report (Form 10-Q) at 21 (July 27, 2017).

be disseminated and the uses to which it will be put is not just a function of technology and the social media it has empowered. To the contrary, credit card issuers,[4] national retail chains,[5] global hotel conglomerates,[6] cable companies,[7] health care providers,[8] and countless other actors in the public sphere all disclose to individuals how and under what circumstances the information they provide may be shared with third parties—and how and to what extent the individual may limit further disclosure of that information (*e.g.*, by precluding a merchant from providing the individual's contact information to a third-party marketing organization).

---

[4] Bank of America, U.S. Consumer Privacy Notice, https://www.bankofamerica.com/privacy/consumer-privacy-notice.go (last visited Aug. 7, 2017).

[5] Macy's, Inc., Macy's and macys.com Notice of Privacy Practices, https://www.customerservice-macys.com/app/answers/detail/a_id/595/session/L2F2LzEvdGltZS8xNTAyMTUwMTAwL3NpZC9IWTdTLUFwbg%3D%3D#pref (last visited Aug. 7, 2017).

[6] InterContinental Hotels Group, InterContinental Hotels Group Privacy Policy, https://www.ihg.com/hotels/gb/en/global/customer_care/privacy_policy#4 (last visited Aug. 7, 2017).

[7] Verizon, Privacy Policy for Fios and Other Fiber-to-the-Premises Customers, http://www.verizon.com/about/privacy/fios-privacy-policy (last visited Aug. 7, 2017).

[8] Kaiser Permanente, Privacy Statement, https://healthy.kaiserpermanente.org/health/care/consumer/ancillary/!ut/p/a1/hZBBj4IwEIV_iwfOM8pGgRuSuFZ0xWgEezEVG2xS26ZOzPLvVYxHw7tN5n1vMg84VMCNuKtGkLJG6NfMx8fZYrueTocprn_iCNkqm2fsL8enoIQF8EbbU2c-XIhcEmCAtTUkDXlpztJLHyDwmlonobopkkdntaqVvPUxZMT1w3Trf-pD_PuMt643XJ2hKosiSZbD_acT1ZpHyLe4cLUSmvh2-f_vKsIQ7bpKvotxogsynf5Ps5DxNHH8EUpgrtGbajvS1lGFLNm8AAgXXxu/dl5/d5/L2dBISEvZ0FBIS9nQSEh/ (last visited Aug. 7, 2017).

5. The above examples highlight just a few facets of what a proper, modern-context-sensitive analysis would look to when attempting to ascertain the reasonableness of an individual's expectation of privacy in his or her cell-site location information. But even this subset of data points shows that societal understandings of privacy have changed significantly from the all-or-nothing concept of information disclosure that appears to undergird *Smith* v. *Maryland*, 442 U.S. 735 (1979), and its progeny. Today, technology has made it possible—and society has deemed it reasonable—for an individual to exert a more nuanced control over the information he or she discloses: *i.e.*, when, where, by whom, and for how long that information may be accessed.

That said, the immediate impact of these changes in societal expectations will be tempered somewhat by the circularity inherent in the *Katz* analysis. *See Kyllo* v. *United States*, 533 U.S. 27, 34 (2001). In other words, the *Katz* test has a locking-in effect: When the Court finds a practice does not trigger the warrant requirement, law enforcement may regularly engage in that process without securing a warrant—a practice that inherently undercuts any societal expectation of privacy in the information the government is securing. Thus, given *Smith*'s holding that the installation of a pen register is not a search, and the resulting ease with which such devices could be deployed, it remains highly unreasonable for an individual to expect such information to remain private.[9]

---

[9] The converse is also true: When the Court holds that a particular practice implicates a reasonable expectation of privacy, that perception of privacy is staunchly reinforced by (1) the reduction in occurrences that necessarily results from requiring a warrant; and (2) the knowledge that a neutral

* * *

In sum, the Court of Appeals failed to apply the methodology required by this Court's cases, eschewing a contemporary-society-based reasonable-expectation-of-privacy analysis (which would have accounted for, *inter alia*, modern technologies and the societal attitudes they impelled) in favor of a rote application of a rule that had its genesis in the heyday of the fax machine and thermal printer. Applying the wrong framework, the court below obtained the wrong answer. As shown above, the correct conclusion is that obtaining 127 days' worth of an individual's cell-site location data is a search within the meaning of the Fourth Amendment. The decision of the Court of Appeals for the Sixth Circuit should therefore be reversed.[10]

II. THE COURT OF APPEALS FAILED TO FACTOR THE NATURE OF THE GOVERNMENT'S REQUEST INTO ITS FOURTH AMENDMENT ANALYSIS.

The Court of Appeals failed to appreciate that the nature and extent of the government's actions—and the use to which that information would be put—had a bearing on its Fourth Amendment analysis. See *Jones*, 565 U.S. at 430-431 (2012) (Alito, J., concurring in the judgment) (contrasting "relatively short-term [GPS] monitoring of a person's movements on public streets," which likely would not qualify as a search,

---

magistrate and standard of probable cause have been interposed between an individual and the executive arm of the state.

[10] Alternatively, the Sixth Circuit's methodological error is, itself, sufficient grounds for vacating that court's decision and remanding this case so that the Court of Appeals may undertake the proper analysis of petitioner's claims.

with "the use of longer term GPS monitoring," which "impinges on expectations of privacy").

Here, the government sought 127 days' worth of petitioner's cell-site location information—effectively putting a retroactive tail on him for more than four months—in order to generate circumstantial evidence that he had, in fact, committed the crimes he was accused of committing. The long-term nature of that surveillance and purpose of gathering information for use in investigating and prosecuting a crime counsel strongly in favor of the conclusion that collection of petitioner's cell-site location information amounted to a search that required a warrant in order to proceed.[11]

The Sixth Circuit's counter-argument—that the information at issue is not specific enough to trench on privacy expectations—is both internally inconsistent and foreclosed by precedent. It is self-contradictory because, despite the supposed imprecision of the location information, it was proffered here—and has been proffered in many other cases—as competent evidence in support of a suspect's prosecution and conviction. *Carpenter*, 819 F.3d at 885; accord *In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d 304, 311-312 (3d Cir. 2010) ("[T]he Government has asserted in other cases that a jury should rely on the accuracy of the cell tower records to infer that an individual, or at least her cell phone, was at home.");

---

[11] A different case might be presented, for example, if the government were to seek a narrower slice of information (*e.g.*, to confirm whether his phone was active or not) over a much more circumscribed period of time (*e.g.*, within a range of a few hours on a particular date) and for a different purpose (*e.g.*, to validate or challenge an alibi defense).

United States v. *Davis*, 785 F.3d 498, 540-541 (11th Cir. 2015) (en banc) (Martin, J., dissenting) (similar).

And the argument is foreclosed because this Court squarely rejected a parallel contention in *Kyllo*. In that case, the Court dismissed out of hand the notion that the lack of specificity in the data being gathered—a "crude visual image" from a thermal camera—precluded a finding that the use of the heat-sensing technology at issue qualified as a Fourth Amendment "search." *Id.* at 36-37. So too here, where the generalized nature of the location information at issue should not be held to insulate the government's collection efforts from the Fourth Amendment's warrant requirement.

Congress affirmed the importance of these contextual factors in its choice of text in Section 2703.

As relevant here, the statute provides:

> **(c) Records Concerning Electronic Communication Service or Remote Computing Service.—**
>
> **(1)** A governmental 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; [or]
>
> **(B)** obtains a court order for such disclosure under subsection (d) of this section; . . . .

Subsection (d), in turn, provides, in relevant part:

> **(d) Requirements for Court Order.—**A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation. . . .

As this text makes plain, Congress mapped out two alternative paths to securing a subscriber's records from an electronic communications service provider: a warrant based on probable cause or a court order based on "reasonable grounds to believe that . . . the records . . . are relevant and material to an ongoing criminal investigation."

Put differently, unless Section 2703(c)(1)(A)'s warrant requirement is entirely superfluous, it must be the case that Congress contemplated that *sometimes* a request for such information would require a warrant, and *sometimes* it would not. Cf. *Corley* v. *United States*, 556 U.S. 303, 314 (2009) (rejecting broad reading of statutory exception to rule excluding certain confessions because that construction would have rendered a different—and narrower—exception provision "nonsensical and superfluous").

The Sixth Circuit's analysis overrides that congressional choice by making an impermissible generalization about the nature of the data that would *never* require a warrant. *Carpenter*, 819 F.3d at 887 ("The business records here fall on the unprotected side of this line. Those records say nothing about the content of any calls. Instead the records include routing information, which the wireless providers gathered in the ordinary course of business. Carriers necessarily track their customers' phones across different cell-site sectors to connect and maintain their customers' calls. And carriers keep records of these data to find weak spots in their network and to determine whether roaming charges apply, among other purposes. Thus, the cell-site data—like mailing addresses, phone numbers, and IP addresses—are information that facilitate personal communications, rather than part of the content of those communications themselves. The government's collection of business records containing these data therefore is not a search."). But, as explained above, that context-bereft analysis is consonant with neither the statutory text nor the Fourth Amendment backdrop against which Congress legislated.

Accordingly, because the Court of Appeals failed to heed the plain text and structure of Section 2703(c) in admitting evidence against Timothy Carpenter that was secured without a warrant, its judgment must be reversed.

CONCLUSION

For the foregoing reasons, the judgment of the Court of Appeals should be reversed.

Respectfully submitted,

JOHN W. WHITEHEAD
DOUGLAS R. MCKUSICK
THE RUTHERFORD INSTITUTE
P.O. Box 7482
Charlottesville, VA 22906
(434) 978-3888

D. ALICIA HICKOK
Counsel of Record
MARK D. TATICCHI
DRINKER BIDDLE & REATH LLP
One Logan Square
Philadelphia, PA 19103
(215) 988-2700
Alicia.Hickok@dbr.com

Counsel for Amicus Curiae

August 14, 2017