In the Supreme Court of the United States

REX HAMMOND,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

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

BRIEF FOR AMICI CURIAE RUTHERFORD INSTITUTE AND THE CATO INSTITUTE IN SUPPORT OF PETITIONER

PAUL J. SAMPSON
Counsel of Record
BRADLEY MASTERS
STEPHEN A. TENSMEYER
KIRKLAND & ELLIS LLP
60 East South Temple
Salt Lake City, UT 84111
(801) 877-8140
paul.sampson@kirkland.com

CLARK M. NEILY III ILYA SHAPIRO CATO INSTITUTE 1000 Mass. Ave., NW Washington, DC 20001 (202) 842-0200 cneily@cato.org

Counsel for Amici Curiae (Additional Counsel Listed on Inside Cover) JOHN W. WHITEHEAD WILLIAM E. WINTERS THE RUTHERFORD INSTITUTE 109 Deerwood Road Charlottesville, VA 22911 (434) 978-3888

JIM HARPER TECHLAW UNIVERSITY OF ARIZONA JAMES E. ROGERS COLLEGE OF LAW 1201 E. Speedway Blvd. Tucson, AZ 85721

TABLE OF CONTENTS

TABLE OF AUTHORITIES	ii
STATEMENT OF INTEREST	. 1
INTRODUCTION AND SUMMARY OF ARGUMENT	
ARGUMENT	. 3
I. The Questions Presented In This Case Are Exceptionally Important In Light Of Recent Technological Developments	. 3
II. The Court Should Grant Certiorari To Correct Legal Errors And Clarify Fourth Amendment Doctrine	. 6
A. Accessing Real-Time CSLI Is a Search Under the Plain Meaning of the Fourth Amendment	. 7
B. The Seventh Circuit Came to an Incorrect Result by Focusing on Doctrinal Glosses Rather than the Original Meaning of the Fourth Amendment	. 8
III. The Government's Conduct Is a Search In Light of Evolving Societal Expectations About Data Privacy	
CONCLUSION	16

TABLE OF AUTHORITIES

Cases
Carpenter v. United States, 138 S. Ct. 2206 (2018)passim
Katz v. United States, 389 U.S. 347 (1967)
Kyllo v. United States, 533 U.S. 27 (2001)
Riley v. California, 573 U.S. 373 (2014)10
State v. Muhammad, 451 P.3d 1060 (Wash. 2019)11
Terry v. Ohio, 392 U.S. 1 (1968)
United State v. Jones, 565 U.S. 400
United States v. Graham, 846 F. Supp. 2d 384 (D. Md. 2012)
United States v Hammond, 996 F.3d 374 (7th Cir. 2021)9, 10
United States v Knotts, 460 U.S. 276 (1983)11, 12
Other Authorities
U.S. CONST. amend. IVpassim
Brian X. Chen, <i>The Battle for Digital Privacy is Reshaping the Internet</i> , NEW YORK TIMES, Sept. 16, 2021
Chris Velazco, Android Privacy Settings to Change Now, WASHINGTON POST, Nov. 29, 2021

Control Over Their Personal Information,	
PEW RESEARCH CENTER	$\dots 15$
CTIA—The Wireless Association, 2021	
Annual Survey Highlights	. 5, 6
Heather Kelly, Apple iOS Privacy Settings to Change Now, WASHINGTON POST, Nov.	
26, 2021	14
Robert McCartney, The Ugly Side of 5G:	
New Cell Towers Spoil the Scenery and Crowd People's Homes, WASHINGTON	
Post, July 12, 2021	6
Simon O'Dea, Market Share of Mobile	
Operating Systems Worldwide 2012-2021	14
STATISTA, June 29, 2021	14

STATEMENT OF INTEREST¹

The Rutherford Institute is an international nonprofit organization headquartered in Charlottesville, Virginia. Founded in 1982 by its President, John W. Whitehead, the Institute provides legal assistance at no charge to individuals whose constitutional rights have been threatened or violated and educates the public about constitutional and human rights issues affecting their freedoms. The Rutherford Institute works tirelessly to resist tyranny and threats to freedom by seeking to ensure that the government abides by the rule of law and is held accountable when it infringes on the rights guaranteed to persons by the Constitution and laws of the United States.

The Cato Institute is a nonpartisan public-policy research foundation established in 1977 and dedicated to advancing the principles of individual liberty, free markets, and limited government. Cato's Robert A. Levy Center for Constitutional Studies was established in 1989 to help restore the principles of limited constitutional government that are the foundation of liberty. Cato's Project on Criminal Justice focuses on the scope of substantive criminal liability, the proper role of police in their communities, the protection of constitutional safeguards for

¹ Pursuant to Supreme Court Rule 37.2(a), amici have provided timely notice to all counsel, and all parties consent to the filing of this brief. Pursuant to Supreme Court Rule 37.6, amici state this brief was not authored in whole or in part by counsel for any party, and that no person or entity other than amici or their counsel made a monetary contribution to fund the preparation or filing of this brief.

criminal suspects and defendants, citizen participation in the criminal justice system, and accountability for law enforcement. Toward those ends, Cato publishes books and studies, conducts conferences, and produces the annual Cato *Supreme Court Review*.

Amici are interested in this case because it deals with core questions of individual liberty protected by the Constitution.

INTRODUCTION AND SUMMARY OF ARGUMENT

When the Kalamazoo police department learned that Rex Hammond was a "person of interest" in a series of armed robberies, Detective Cory Ghiringhelli submitted a request to AT&T, Hammond's wireless carrier, to generate and obtain real-time cell site location information ("CSLI") to locate Hammond. AT&T "pinged" Hammond's cell phone, which generated a record of the location of Hammond's phone. AT&T then provided this newly created record to Ghiringhelli, who used it to locate Hammond and obtain evidence that was later used to convict him.

The Seventh Circuit held that Detective Ghiringhelli's warrantless collection of real-time CSLI did not constitue a search. In so holding, the Seventh Circuit distinguished this Court's holding in Carpenter v. United States, 138 S. Ct. 2206 (2018), which did not reach the constitutionality of obtaining real-time CSLI without a warrant. *Id.* at 2220.

If allowed to stand, the decision below will have grave consequences for privacy interests protected by the Fourth Amendment. Americans have become increasingly reliant on their cell phones. At the same time, recent technological developments have boosted cell phone providers' ability to obtain accurate real-time data on their users' whereabouts. Absent constitutional guardrails, this confluence effectively empowers law enforcement to locate any individual in the United States at any time within a few feet without the constraints of traditional tools for tracking and surveilling.

This Court should grant Hammond's Petition for a Writ of *Certiorari* (the "Petition") to reaffirm that the ultimate test of whether government conduct constitutes a search is the language of the Fourth Amendment itself. *See* U.S. Const. amend. IV. Applying those terms, the government's conduct here was a straightforward search of Hammond's "person[]" and "effects," and its failure to obtain a warrant before conducting that search rendered it unreasonable. Moreover, even under the existing "reasonable expectations of privacy" test, the government's conduct constitutes a search in light of society's evolving expectation toward enhanced data privacy.

ARGUMENT

I. The Questions Presented In This Case Are Exceptionally Important In Light Of Recent Technological Developments

A person's location offers "an intimate window" into that person's life, "revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations." *Carpenter*, 138 S. Ct. at 2217 (internal quotation marks omitted). That is true equally of data

revealing a person's historical location (as in *Carpenter*) and a person's real-time location (as in this case). By accessing location data, the government can "achieve[] near perfect surveillance, as if it had attached an ankle monitor to the phone's user." *Id.* at 2218. The Constitution's protections must remain functional notwithstanding the unrelenting drumbeat of technological progress, and the fundamental rights of Americans must not be thrown "at the mercy of advancing technology." *Kyllo v. United States*, 533 U.S. 27, 35 (2001).

Modern cell phones contain a "vast store of sensitive information." *Carpenter*, 138 S. Ct. at 2214, 2218. And as Americans become more and more reliant on their phones to conduct the business of their daily lives, this store of information is ever-growing. "Over the past decade, Americans have driven a 108x increase in mobile data traffic," including "a ~207% increase since 2016" to a total of approximately 42 trillion megabytes of data traffic in 2020.²

Among the stores of information collected or conveyed by cell phones, personal location data is among the most revealing and private. *Carpenter*, 138 S. Ct. at 2217 ("These location records hold for many Americans the privacies of life." (internal quotation marks omitted)). In *Carpenter*, the Court noted that "[a]s the number of cell sites has proliferated" and "the geographic area covered by each cell sector has

 $^{^2}$ CTIA—The Wireless Association, 2021 Annual Survey Highlights ("CTIA 2021 Survey") at 8, available at https://bit.ly/31ZStLS.

shrunk," the accuracy of CSLI in pinpointing an individual's precise location has increased. 138 S. Ct. at 2219. In the few short years since *Carpenter* was decided, the pace of these changes has only quickened, and the privacy implications of accessing real-time CSLI have increased dramatically.

Most notably, in 2019, "5G" networks were introduced and began a rapid nationwide rollout.³ The CSLI associated with these 5G networks has the potential to be much more revealing than the CSLI associated with 3G or 4G networks. As compared to these earlier networks, 5G networks use "higher-frequency radio waves, which carry much more data but have shorter ranges." 5G networks therefore require a much denser collection of cell sites than has previously existed. As a result, the number of cell sites has increased dramatically since 5G was introduced in 2019. "By the end of 2020, over 417,000 cell sites were built and operational, an increase of 35% since 2016[.]" 5

This shorter range and denser network of cell sites means that CSLI data can pinpoint a person's location with much greater precision than ever before, particularly if law enforcement uses "triangulation methods" that determine the time and angle of a

³ CTIA 2021 Survey at 7 ("5G...already cover[s] 300 million Americans, up from 200 million last year and amounting to over 90% of the entire country. 5G networks are also being built out and expanding faster than 4G.") (emphasis omitted).

⁴ Robert McCartney, *The Ugly Side of 5G: New Cell Towers Spoil the Scenery and Crowd People's Homes*, WASHINGTON POST, July 12, 2021, *available at* https://wapo.st/3qaEMBP.

⁵ CTIA 2021 Survey at 5 (emphasis omitted).

device with respect to multiple nearby cell sites. *Carpenter*, 138 S. Ct. at 2219 (citing Brief for Electronic Frontier Foundation et al. as *Amici Curiae* 12). The Court's prediction in *Carpenter* that "the accuracy of CSLI is rapidly approaching GPS-level precision" has already become reality in many parts of the country. *Id.* The privacy issues raised in this case are therefore of acute and increasing importance and counsel in favor of granting the Petition.

II. The Court Should Grant Certiorari To Correct Legal Errors And Clarify Fourth Amendment Doctrine

Americans' increasing reliance on cell phones heightens the risk of unwarranted government intrusion into their privacy. When the government requests cell phone providers to uncover a person's real-time location, the government is conducting a search. In this case, the government likely could have demonstrated probable cause to obtain a search warrant. Enforcing the Fourth Amendment's prohibition against warrantless searches thus would not have impeded the Kalamazoo police department's investigation. But if the government is not required to obtain a search warrant in order to gather real-time location data from cell phone providers, then government agents could track almost anyone who has a cell phone without having probable cause to do so. Thus, clarifying the law will protect Americans from real-time invasions of their privacy going forward.

A. Accessing Real-Time CSLI Is a Search Under the Plain Meaning of the Fourth Amendment

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated[.]" U.S. CONST. amend. IV. In accordance with this language, the appropriate analysis in this case is to ask whether there was a search or seizure, whether this search or seizure was of "persons, houses, papers, [or] effects," and whether the search or seizure was reasonable. See, e.g., Terry v. Ohio, 392 U.S. 1, 19 (1968) (conducting a Fourth Amendment analysis in this manner).

When the Fourth Amendment was adopted, as now, to "search" meant "[t]o look over or through for the purpose of finding something; to explore; to examine by inspection; as, to *search* the house for a book; to *search* the wood for a thief." *Kyllo v United States*, 533 U.S. 27, 32 n.1 (2001) (quoting N. Webster, An American Dictionary of the English Language 66 (1828) (reprint 6th ed. 1989)) (emphasis in original). Because the Fourth Amendment is a limitation on *government* conduct, the focus of the constitutional inquiry should be on the nature and purpose of the government's conduct.

Focusing on the government's conduct yields an easy answer in this case. Law enforcement conducted a search of Hammond's person and effects by "pinging" his cell phone and accessing the nonpublic data generated in response with the specific purpose of locating him wherever he happened to be—whether at

home or elsewhere. There is no need to conduct a circuitous inquiry that evaluates the government's actions against the subjective expectations of Hammond or the objective expectations of society at large.

В. The Seventh Circuit Came an Incorrect Result **Focusing** by on than **Doctrinal** Glosses Rather the Original Meaning of the Fourth Amendment

Although the answer in this case ultimately is the same regardless of whether the Fourth Amendment's text or the reasonable expectations of privacy test guides the inquiry, taking the perilous path outlined by the *Katz* test can easily lead one down blind alleys. It often obscures what it is supposed to clarify. Indeed, this is precisely what happened in the decision below. By focusing exclusively on the *Katz* test, the Seventh Circuit wound up relying on distinctions without a difference and principles without any grounding in the Fourth Amendment.

For example, in ruling that no search occurred, the Seventh Circuit relied on the fact that "[l]aw enforcement used the real-time CSLI to find Hammond's location in public, not to peer into the intricacies of his private life." *United States v Hammond*, 996 F.3d 374, 389 (7th Cir. 2021) ("Hammond does not argue that he was in private areas during this time period."). The fact that Hammond happened to be traveling "on public, interstate highways and into parking lots within the public's view" at the time the government pinged his phone is merely fortuitous. He could just as easily

have been at home, or at his girlfriend's home, or at a political event.

The Seventh Circuit's focus on the results of the government's action, rather than the nature of the action itself, led it to a purely retrospective rule that turns the protections afforded by the Fourth Amendment into a game of roulette. If the Fourth Amendment is to guide government conduct or provide any protection to citizens, the government must be able to know whether a particular action is a search before taking it. Defining the same action as a search based on what it happens to reveal is not theoretically or practically workable. See Riley v. California, 573 U.S. 373, 398 (2014) ("[I]f police are to have workable rules, the balancing of the competing interests . . . must in large part be done on a categorical basis—not in an ad hoc, case-by-case fashion by individual police officers.") (internal quotation marks omitted).

As explained in *Carpenter*, "[a] cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." 138 S. Ct. at 2218. In this case, when the police pinged Hammond's cell phone, they had no idea where he was or how private that location might be. Indeed, they conducted the search precisely because they did not know where he was.

The Seventh Circuit found itself down another doctrinal rabbit-hole when it attempted to distinguish *Carpenter* on the basis that the police in this case tracked Hammond in real time "over the course of several hours" rather than over multiple days. 996 F.3d at 390. The Seventh Circuit claimed that this

limited duration made this case more similar to *United States v Knotts*, 460 U.S. 276 (1983), than to *Carpenter*. Again, the distinctions made by the Seventh Circuit are irrelevant to the terms of the Fourth Amendment.

There is no relevant difference—whether in terms of societal expectations of privacy or of the nature of actions—between the government's tracking someone's location over a period of time and tracking that person's location at any given time. State v. Muhammad, 451 P.3d 1060, 1073 (Wash. 2019) ("[T]o conclude that one cell phone ping is not a search, provided it lasts less than six hours, yet hold multiple or longer pings do qualify as search is not a workable analysis."); United States v. Graham, 846 F. Supp. 2d 384, 401 (D. Md. 2012) ("[T]he law as it now stands simply does not contemplate a situation whereby traditional surveillance becomes Fourth Amendment 'search' only after some specified period of time—discrete acts of law enforcement are either constitutional or they are not.").

In any event, the government's search of Hammond in this case is fundamentally different from the conduct in *Knotts*. In *Knotts*, police identified a person of interest and were able to track him only after they first located him through ordinary questioning and observation. See 460 U.S. at 278 (noting that law enforcement determined where the defendant would chloroform drum through purchase "[vlisual surveillance"). In other words, in *Knotts* the police used technology only to *maintain* contact over a brief period after they first established that contact through old-fashioned visual surveillance. Id. ("[O]fficers

followed the car in which the chloroform had been placed, maintaining contact by using both visual surveillance and a monitor which received the signals sent from the beeper."). Further, officers knew that the person of interest in *Knotts* would be tracked while travelling on public roads after he purchased the choloroform. *Id.* In contrast, CSLI allows police to establish contact in the first instance, regardless of where the person happens to be.

This confusion could have been avoided if the Seventh Circuit's inquiry focused on what the Fourth Amendment focuses on—the government's action. The police used a technological capability "not in general public use" for the purpose of surveilling Hammond and bringing out of concealment a private detail of his life. *Kyllo v. United States*, 533 U.S. 27, 40 (2001). This "surveillance is a 'search' and is presumptively unreasonable without a warrant." *Id.* Because there are no circumstances that excuse law enforcement's failure to obtain a warrant based on probable cause, that search was unreasonable and violated the Fourth Amendment.

III. The Government's Conduct Is a Search In Light of Evolving Societal Expectations About Data Privacy

Even if the Court applied the reasonable expectation of privacy test from Justice Harlan's concurrence in *Katz v. United States*, 389 U.S. 347 (1967), the government action at issue here would be a search, and conducting that search without a warrant would violate the Fourth Amendment. In apparent backlash against the revelation that third parties collect staggering amounts of data on

individual cell phone users, societal expectations have shifted toward cell phone users having and expecting greater control over their personal data. In particular, individuals increasingly retain control over who can learn their physical location at any given time. These evolving expectations demonstrate that society recognizes a reasonable privacy interest in real-time CSLI and that warrantless searches of such data invade that interest in violation of the Fourth Amendment.

Although the *Katz* test asks courts to evaluate society's expectations about privacy, these expectations are not static. In particular, "[d]ramatic technological change . . . may ultimately produce significant changes in popular attitudes." *United State v. Jones*, 565 U.S. 400, 427 (Alito, J., concurring in the judgment); *see also id.* at 415 (Sotomayor, J., concurring) (noting the "evolution of societal privacy expectations" in light of "technological advances").

But technological change does not always move in the direction of *lower* expectations of privacy. Indeed, as cell phone capabilities have increased, technology companies have given users *more* control over what types of data are collected and how they are used. ⁶ Of particular relevance here, cell phone users are accustomed to granting or denying permission to access location data on an app-by-app basis. Both the Android and Apple operating systems—which

⁶ See Brian X. Chen, The Battle for Digital Privacy is Reshaping the Internet, NEW YORK TIMES, Sept. 16, 2021, available at https://nyti.ms/3yJz8dB.

together represent more than 99% of the cell phone market⁷—allow for these fine-grained controls over how location data is shared.⁸

As a result of these changes and the public preferences that prompted them, today cell phone users can reasonably expect that they control when and by whom their location is tracked. Indeed, polling by the Pew Research Center conducted in June 2019 showed that nearly three-quarters of Americans felt they had either "a lot" or at least "a little" control over who could learn their physical location. This was the highest level of perceived control reported for any category of personal information on the survey, and it is significantly higher than the proportion of respondents who reported feeling any level of control over other categories of information such as search

⁷ Simon O'Dea, Market Share of Mobile Operating Systems Worldwide 2012-2021, STATISTA, June 29, 2021, available at https://bit.ly/3yzJSeB.

⁸ Heather Kelly, Apple iOS Privacy Settings to Change Now, WASHINGTON Post, Nov. 26, 2021, availablehttps://wapo.st/321Yp74 ("Think of your location as one of the most sensitive categories of information. It can reveal where you live and work, what businesses or doctors you frequent and if you go any place sensitive like a protest. You can turn off Location Services and revoke access for all apps[.]"); Chris Velazco, Android Privacy Settings to Change Now, WASHINGTON POST, Nov. 29, 2021, available at https://wapo.st/3p5SFSr ("Go to Settings → Privacy → Permissions Manager; you'll see a list of options ranging from body sensors to location to your contacts. Tap each option and make sure the 'allowed' apps make sense[.]").

⁹ Brooke Auxier et al., Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information, PEW RESEARCH CENTER at 23, Nov. 15, 2019.

terms they used online (48%), websites they visited (54%), or even private conversations such as text messages (62%). ¹⁰ In other words, Americans feel they have *more* control over their physical location than they do over unquestionably protected information such as private conversations.

The mere fact that cell service providers can obtain data on their users' whereabouts does not vitiate this expectation of privacy. As this Court has recognized, "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data" to the providers. Carpenter, 138 S.Ct. at 2220. Thus, while individuals increasingly retain control over which third-party device and app providers have access to their location data, they cannot hide their location from cell service providers without forgoing cell phone use altogether. Neither the Constitution nor the *Katz* test forces individuals to choose between their cell phones and their privacy rights. Instead, the inquiry should focus on the fact that in those instances in which retaining control over one's location is possible, society expects users to have control over who is allowed to know their location.

As discussed above, no doctrinal inquiry into society's expectations is necessary to reach the conclusion that "pinging" a cell phone to generate real-time CSLI constitutes a search. Nevertheless, such an inquiry confirms that users have a heightened sense that their location at any given time is a private

 $^{^{10}}$ *Id*.

matter over which they have some control, and they certainly do not expect police to be tracking their current location and movements through their cell phones without a search warrant. Accessing real-time CSLI invades that reasonable expectation of privacy and thus constitutes a search under the Fourth Amendment. The Court should grant the Petition to confirm these societal expectations and protect Americans' justified perception that they control at least some aspect of their digital lives from government intrusion.

As this Court has held, a central aim of the Fourth Amendment was "to place obstacles in the way of a too permeating police surveillance." *Carpenter*, 138 S. Ct. at 2214 (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)). It is difficult to imagine a more "permeating police surveillance" than the ability to determine any person's location at any given time. And as explained above, cell phone users do not accept such surveillance as a necessary trade-off in exchange for the benefits of these devices. Instead, they increasingly expect that they control such data and who has access to it.

The Court should grant the Petition to vindicate cell phone users' reasonable expectations and, at the same time, clarify that these expectations are not necessary to determine that what occurred here was an unreasonable search. Although some forms of location information may reveal only a person's general whereabouts, more precise location data can show exactly whom the person associated with, which buildings or even rooms of buildings the person entered, or which sections of a library he visited. When

the government sets out to learn a person's precise location and reveals such data, it conducts a search within the meaning of the Fourth Amendment. In this case, the police conducted a search when they targeted Hammond and generated new data from a device he owned to bring his location out of concealment. To do so without a warrant based on probable cause was unreasonable.

CONCLUSION

For the foregoing reasons, the Petition should be granted and the decision below should be reversed.

Respectfully submitted,

Paul J. Sampson
Counsel of Record
Bradley Masters
Stephen A. Tensmeyer
KIRKLAND & ELLIS LLP
60 East South Temple
Salt Lake City, UT 84111
(801) 877-8140
paul.sampson@kirkland.com
John W. Whitehead
William E. Winters
THE RUTHERFORD
INSTITUTE

CLARK M. NEILY III
ILYA SHAPIRO
CATO INSTITUTE
1000 Mass. Ave., NW
Washington, DC 20001
(202) 842-0200
cneily@cato.org

JIM HARPER
TECHLAW
UNIVERSITY OF
ARIZONA
JAMES E. ROGERS
COLLEGE OF LAW
1201 E. Speedway Blvd.
Tucson, AZ 85721

Counsel for Amici Curiae

December 20, 2021

109 Deerwood Road

(434) 978-3888

Charlottesville, VA 22911