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 FOR PETITIONER

Nathan Freed Wessler
Ben Wizner
Brett Max Kaufman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
New York, NY 10004

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

Cecillia D. Wang
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111

Harold Gurewitz
Counsel of Record
GUREWITZ & RABEN, PLC
333 W. Fort Street, Suite 1400
Detroit, MI 48226
(313) 628-4733
hgurewitz@grplc.com

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

Jeffrey L. Fisher
STANFORD LAW SCHOOL SUPREME COURT LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305

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.

PARTIES TO THE PROCEEDINGS

In addition to the parties named in the caption, Timothy Michael Sanders was a defendant–appellant below, and was represented by separate counsel.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

CONSTITUTION & STATUTES

LEGISLATIVE MATERIALS

OTHER AUTHORITIES

BRIEF FOR PETITIONER

Petitioner Timothy Carpenter respectfully requests that this Court reverse the judgment of the United States Court of Appeals for the Sixth Circuit.

OPINIONS BELOW

The opinion of the Sixth Circuit (Pet. App. 1a-32a) is reported at 819 F.3d 880. The district court opinion (Pet. App. 34a-48a) is unpublished, but is available at 2013 WL 6385838.

JURISDICTION

The Sixth Circuit issued its opinion on April 13, 2016, and denied rehearing en banc on June 29, 2016. Pet. App. 33a. This Court has jurisdiction pursuant to 28 U.S.C. § 1254(1).

RELEVANT CONSTITUTIONAL AND STATUTORY PROVISIONS

The Fourth Amendment to the U.S. Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Stored Communications Act, 18 U.S.C. § 2703, provides in relevant part:

(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; * * *

(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 contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. * * *

STATEMENT OF THE CASE

1. This case concerns governmental acquisition of personal location records, known as cell site location information ("CSLI"), to identify Petitioner Timothy Carpenter's whereabouts over more than four months. The records, which are logged and retained by cellular service providers whenever people carry modern cell phones, make it possible to reconstruct in detail everywhere an individual has traveled over hours, days, weeks, or months.

In order to access the cellular network, cell phones must connect to nearby cell towers (known as "cell sites"), thereby creating a record of the phone's location. The precision of a cell phone user's location reflected in CSLI records depends on the size of the cell site "sectors" in the area. Most cell sites consist of multiple directional antennas that divide the cell site into sectors. Pet. App. 5a. The majority of cell sites comprise three directional antennas that divide the cell site into three sectors (usually 120 degrees each), but an increasing number of towers have six antennas (covering approximately 60 degrees each). Pet. App. 14a; *see also* Joseph Hoy, *Forensic Radio Survey Techniques for Cell Site Analysis* 61 (2015). The coverage area of each cell site sector is smaller in areas with greater density of cell sites, with urban areas having the greatest density and thus the smallest coverage areas. Pet. App. 5a; *see also* Pet. App. 87a (Gov't Trial Ex. 57, at 13) (providing maps of MetroPCS and Sprint cell sites). The smaller the coverage area, the more precise the location information revealed and recorded.

The density of cell sites continues to increase as data usage from smartphones grows. Because each

cell site carries a fixed volume of data required for text messages, emails, web browsing, streaming video, and other uses, as smartphone data usage increases, carriers erect additional cell sites, each covering smaller geographic areas. *See* CTIA, *Annual Wireless Industry Survey* 4 (2017)[1] (number of cell sites in the United States increased from 195,613 to 308,334 from 2006 to 2016); *id.* at 3 (annual wireless data usage increased more than 3,500 percent from 2010 to 2016). This means that in urban and dense suburban areas like Detroit, many sectors cover small geographic areas. Pet. App. 5a.

Service providers have long retained location information for the start and end of incoming and outgoing calls. Pet. App. 5a-6a. Today, those companies increasingly also retain location information related to the transmission of text messages and routine internet connections—which smartphones make virtually constantly to check for new emails, social media messages, weather updates, and other functions. *See* Craig Silliman, Exec. Vice President, Pub. Pol'y & Gen. Counsel, Verizon, *Technology and Shifting Privacy Expectations*, Bloomberg Law, Oct. 7, 2016.[2] The information recorded can include not only cell site and sector, but also estimated distance of the phone from the nearest cell site. *Id.* Location precision is also increasing as service providers deploy millions of "small cells," "which cover a very specific area, such as one floor of

---

[1] https://www.ctia.org/docs/default-source/default-document-library/annual-year-end-2016-top-line-survey-results-final.pdf.

[2] https://bol.bna.com/technology-and-shifting-privacy-expectations-perspective.

a building, the waiting room of an office, or a single home." *United States v. Graham*, 824 F.3d 421, 448 (4th Cir. 2016) (en banc) (Wynn, J., dissenting in part and concurring in the judgment) (citation omitted); *see also* Hoy, *supra*, at 69-70.

All told, a typical smartphone connects to cell towers hundreds of times a day, generating a densely pixelated matrix of data points documenting the user's movements. The volume and precision of that data will grow steadily in coming years, generating ever more granular locational information.

Congress has explicitly recognized the sensitivity of CSLI. The Telecommunications Act treats this data as proprietary to the customer, and bars cellular service providers from sharing a customer's CSLI without the customer's express advance approval. 47 U.S.C. § 222(c)(1)-(2), (f).

2. In 2011, officers from the Detroit Police Department arrested four individuals they thought had robbed Radio Shack and T-Mobile stores in Detroit, Michigan. Pet. App. 53a. One of the arrestees "admitted he had a role in eight different robberies that started in December of 2010 and lasted through March of 2011 at Radio Shack and T-Mobile stores in Michigan and Ohio. . . . The [arrestee] identified 15 other individuals who had been involved in at least one of the eight robberies." Pet. App. 53a-54a.

An Assistant United States Attorney then submitted three applications for orders to access 152 days of historical cell phone location records for Timothy Carpenter and several other suspects. Pet. App. 3a, 49a-55a, 62a-68a. The applications, which

were unsworn, did not seek warrants based on probable cause, but rather orders under a 1986 law, the Stored Communications Act ("SCA"), 18 U.S.C. § 2703(d). SCA orders may issue when the government "offers specific and articulable facts showing that there are reasonable grounds to believe that" the records sought "are relevant and material to an ongoing criminal investigation." *Id.*

The primary application at issue here asserted that "the requested records will assist in identifying and locating the other individuals believed to be involved in the armed robberies" and "provide evidence that . . . Timothy Carpenter and other known and unknown individuals are violating provisions of Title 18, United States Code, §1951." Pet. App. 54a. The application sought "[a]ll subscriber information, toll records and call detail records . . . from [the] target telephones from December 1, 2010 to present[,]" as well as "cell site information for the target telephones at call origination and at call termination for incoming and outgoing calls[.]" Pet. App. 4a (some alterations in original); *see also* Pet. App. 52a.

Magistrate judges issued two separate orders granting the applications for Carpenter's records. Pet. App. 56a-61a, 69a-73a. (The third order, also granted, sought CSLI of other suspects). The first order directed MetroPCS, Carpenter's cellular service provider, to "provide the locations of cell/site sector (physical addresses) for the target telephones at call origination and at call termination for incoming and outgoing calls" from "December 1, 2010 to present [May 2, 2011]." Pet. App. 59a-61a. MetroPCS complied, providing 186 pages of Carpenter's cell

phone records (known as "call detail records") to the government.[3] Those records show the cell site and sector that Carpenter's phone connected to at the start and end of most of his incoming and outgoing calls over the course of 127 days.[4] Pet. App. 5a-7a.

The second order directed Sprint to produce cell site location information for Carpenter's phone while it was "roaming on Sprint's cellular tower network" for seven days in March, 2011. Pet. App. 72a. "Metro PCS does not have coverage in the Warren, Ohio area," where one of the charged robberies took place, and has a "roaming agreement . . . with Sprint, which does cover that area." J.A. 63. Therefore, Sprint, not MetroPCS, possessed Carpenter's CSLI for his time spent in and around Warren. Sprint produced two days' worth of CSLI.

MetroPCS and Sprint also produced lists of their cell sites in southern Michigan and northwestern Ohio, respectively, providing the longitude, latitude, and physical address of each cell site, along with the directional orientation of each sector antenna. *See* J.A. 79. Cross-referencing the information in Carpenter's call detail records with

---

[3] Two pages from Carpenter's records were introduced at trial. J.A. 135-36 (Defendant's Trial Exs. 2 & 3). The government provided the full records to the defense in discovery and a prosecution witness discussed them at trial. J.A. 50-51. The full CSLI records were filed as an appendix to the Amicus Brief of the American Civil Liberties Union et al. at the Sixth Circuit. *See* 6th Cir. Doc. No. 33-1.

[4] Although the government's application and resulting court order sought 152 days of records, MetroPCS produced 127 days of records.

these cell site lists allowed law enforcement to identify the area in which Carpenter's phone was located and thereby to deduce Carpenter's location and movements over the course of each day.

All told, the government obtained 12,898 CSLI data points tracing Carpenter's movements—an average of 101 location points per day for more than four months' time. 6th Cir. Doc. No. 29, at 9.

3. Before trial, Carpenter moved to suppress the CSLI records on the basis that the Fourth Amendment prohibits their acquisition without probable cause and a warrant. Pet. App. 36a-37a; *see also id.* at 4a. The district court denied the motion, reasoning that people do not have a reasonable expectation of privacy in CSLI records—and, consequently, their acquisition by the government does not constitute a "search" under the Fourth Amendment. Pet. App. 38a-39a.

At trial, FBI Special Agent Christopher Hess testified that Carpenter's CSLI placed him near four of the charged robberies. Pet. App. 5a-6a. Hess produced maps, constructed using the CSLI, which showed the location of Carpenter's phone relative to the locations of the robberies. Pet. App. 6a; *id.* at 85a-89a (Gov't Trial Ex. 57). The government relied on the records to show Carpenter's proximity to "the robberies around the time the robberies happened." Pet. App. 6a. The prosecutor argued to the jury, for example, that Carpenter was "right where the first robbery was at the exact time of the robbery, the exact sector," J.A. 131, and that he was "right in the right sector before the RadioShack [robbery] in Highland Park," J.A. 132; *see also* J.A. 53-67 (testimony of Special Agent Hess).

The jury convicted Carpenter of six robberies in violation of the Hobbs Act, 18 U.S.C. § 1951(a), and five separate violations of 18 U.S.C. § 924(c) for using or carrying a firearm in connection with a federal crime of violence and aiding and abetting the commission of that offense. The court sentenced Carpenter to nearly 116 years' imprisonment.

4. A divided panel of the Sixth Circuit affirmed. The panel majority acknowledged that in *United States v. Jones*, 565 U.S. 400 (2012), five Justices agreed that people have a reasonable expectation of privacy in information very similar to the CSLI data obtained here—namely, "longer term GPS monitoring in government investigations of most offenses." Pet. App. 13a (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring in the judgment)). But the majority held that individuals have no reasonable expectation of privacy in cell phone location records. Pet. App. 17a. It distinguished *Jones* on the ground that "[t]his case involves business records obtained from a third-party," Pet. App. 14a, which the majority viewed as more like the landline calling records that this Court held in 1979 were not entitled to Fourth Amendment protection, Pet. App. 11a-12a (citing *Smith v. Maryland*, 442 U.S. 735 (1979)). The majority also noted that the GPS information in *Jones* was "accurate enough to show that the target [was] located within an individual building," while CSLI was less precise. Pet. App. 14a-15a.

Judge Stranch disagreed. Concurring in the judgment only, she explained that "the sheer quantity of sensitive information procured without a warrant in this case raises Fourth Amendment

concerns of the type the Supreme Court . . . acknowledged in [*Jones*]." Pet. App. 24a. "I do not think that treating the CSLI obtained as a 'business record' and applying that test addresses our circuit's stated concern regarding long-term, comprehensive tracking of an individual's location without a warrant." *Id.* at 29a. Judge Stranch concluded, however, that suppression was not warranted under the good-faith exception to the exclusionary rule, a question that the majority did not address. *Id.* at 29a-31a.

SUMMARY OF ARGUMENT

I. Under this Court's recent Fourth Amendment cases, the government conducted a search when it obtained 127 days of petitioner's cell phone location records from his cellular service provider.

A. When the government employs new technology to obtain sensitive personal information in a way that diminishes the degree of privacy that individuals reasonably expected prior to the technology's adoption, it conducts a search under the Fourth Amendment. Applying this principle in *United States v. Jones*, 565 U.S. 400 (2012), five Justices concluded that longer-term GPS tracking of a car violates reasonable expectations of privacy. Tracing a person's geographical movements reveals highly sensitive personal information, and prior to the digital age, people reasonably expected that police in most investigations would not have followed a person and recorded her every movement for days or weeks on end.

The same analysis controls this case. CSLI exposes a great volume of highly sensitive information about a person, revealing where she has been and whom she has been with throughout each day. And as acute as that concern is today, it will only sharpen over time, as the volume and precision of CSLI records steadily increases. Furthermore, just as with GPS tracking, the government prior to the widespread proliferation of cell phones could have obtained only very limited information about a person's past geographical movements. Police officers could have, for example, interviewed witnesses, sought security camera footage, or examined store receipts near the scene of a crime. But these tactics pale in comparison to the unprecedented surveillance time machine that CSLI provides.

In addition, obtaining CSLI records invades an individual's Fourth Amendment right to security in his private "papers." Federal law grants individuals a proprietary interest in their CSLI records by prohibiting service providers from disclosing that information without "express prior authorization of the customer." 47 U.S.C. § 222(f). Wholly apart from a reasonable-expectation-of-privacy analysis, the government's impingement on that interest for purposes of gathering information constitutes a search.

B. Contrary to the Sixth Circuit's view, decades-old cases involving the "third-party doctrine" do not render the Fourth Amendment inapplicable here. In *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976), this Court concluded that people lack a reasonable expectation of privacy in dialed telephone numbers

and banking records, because of the records' limited sensitivity and because the information involved was voluntarily conveyed to third parties. But a great gulf divides those cases from the investigative activity at issue here.

The detailed and pervasive location records obtained in this case are far more comprehensive and sensitive than discrete telephonic or banking information. And location data is not "voluntarily" conveyed by a phone user in the same sense as the information in *Smith* and *Miller*. Cell phones are indispensable to participation in modern society—often required for employment, relied on for personal safety, and increasingly becoming essential medical treatment tools. Even if it could be said that *possessing* a cell phone is a voluntary act, it certainly cannot be said that cell phone owners knowingly and intentionally disclose their minute-by-minute movements in historical perpetuity. Carrying a smartphone, checking for new emails from one's boss, updating the weather forecast, and downloading directions ought not license total surveillance of a person's entire life.

As this Court's decisions in *Jones*, 565 U.S. 400, and *Riley v. California*, 134 S. Ct. 2473 (2014), illustrate, the innovations of the digital age preclude wooden extension of analog-era precedents where technology has greatly increased the government's ability to obtain intimate information. Extending *Smith* and *Miller* to CSLI would lead to unacceptable consequences. It would mean not only that CSLI is exempt from the Fourth Amendment, but also that persons would lack any reasonable expectation of privacy in the contents of emails and other

communications that are necessarily shared with service providers to enable their transmission. People reasonably expect that the details of where they travel over an extended period are known only to themselves, and therefore cannot be obtained by the government without implicating the Fourth Amendment.

II. This Court may wish to allow the Sixth Circuit to determine in the first instance whether a search of CSLI pursuant to an order under the Stored Communications Act is "reasonable" under the Fourth Amendment. Should the Court reach the question, however, it should hold that such a search is unreasonable.

The usual rule is that a warrant is required for criminal investigative searches. And Congress has not decreed here to the contrary. Congress enacted the SCA prior to the widespread proliferation of cell phones and without awareness of the coming availability of CSLI.

Nor does any exception to the warrant requirement apply here. The government argues that its subpoena power allows it to obtain CSLI records on a showing of less than probable cause. But the subpoena power allows the government merely to obtain business records in which businesses have a diminished expectation of privacy, if they have any at all. This Court has never extended that power to records as to which individuals have a reasonable expectation of privacy. And allowing warrantless access to such information—particularly CSLI records—would constitute a massive expansion of government power and a threat to personal privacy

akin to the general warrants that the Framers of the Fourth Amendment so abhorred.

ARGUMENT

I. THE ACQUISITION OF LONGER-TERM CELL SITE LOCATION INFORMATION CONSTITUTES A SEARCH.

The Sixth Circuit held—and the government argues—that the Fourth Amendment does not restrict access to CSLI because it involves no "search" or "seizure." If the Court were to accept this argument, the government could use this tool to monitor the minute-by-minute whereabouts of anyone—from ordinary citizens to prominent businesspersons to leaders of social movements. The implication of the government's position is not that it should be able to obtain CSLI about particular suspects in particular investigations pursuant to orders under § 2703(d) of the Stored Communications Act; Congress could repeal that statute tomorrow. Rather, it is that the government could obtain every American's location history detailing their movements 24 hours a day, seven days a week, month after month, with no quantum of suspicion or judicial oversight whatsoever. That sweeping proposition is incompatible with the requirements of the Fourth Amendment.

A. Individuals Have A Reasonable Expectation Of Privacy In Their Longer-Term Cell Phone Location Records.

1. Under this Court's longstanding test, government agents engage in a Fourth Amendment

search when they intrude on an expectation of privacy that society is prepared to recognize as reasonable. *Kyllo v. United States*, 533 U.S. 27, 33 (2001); *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The touchstone for determining when an expectation of privacy is reasonable is "the everyday expectations of privacy that we all share." *Minnesota v. Olson*, 495 U.S. 91, 98 (1990). For example, this Court held in *Katz* that the Fourth Amendment applies to conversations transmitted over telephone lines because phones played a "vital role" in conducting the type of communication previously treated as "private." 389 U.S. at 352-53.

As new technology has dramatically lowered the cost of government surveillance and increased the government's access to private information, this Court has stressed that the reasonable-expectation-of-privacy inquiry must "assur[e] preservation of that degree of privacy against government that existed" prior to the advent of the new technology in question. *United States v. Jones*, 565 U.S. 400, 406 (Scalia, J.) (alteration in original); *id.* at 420 (Alito, J., concurring in the judgment); *Kyllo*, 533 U.S. at 34; *see also Riley v. California*, 134 S. Ct. 2473, 2490 (2014) (requiring a warrant to search contents of cell phones seized incident to arrest in order to preserve degree of privacy enjoyed before invention and pervasive use of cell phones).

Applying this framework in *United States v. Jones*, five Justices agreed that people have a reasonable expectation of privacy in "longer term GPS monitoring in investigations of most offenses." *Jones*, 565 U.S. at 430 (Alito, J., concurring in the

judgment); *id.* at 415 (Sotomayor, J., concurring). Because GPS monitoring of a car tracks "every movement" a person makes in that vehicle, *id.* at 430 (Alito, J., concurring in the judgment), it generates extremely sensitive and private information that "enables the Government to ascertain, more or less at will, [people's] political and religious beliefs, sexual habits, and so on," *id.* at 416 (Sotomayor, J., concurring). Prior to the digital age, this information would have been largely immune from search. Although historically the government could have tasked a team of agents with surreptitiously tailing a suspect, doing so "for any extended period of time was difficult and costly and therefore rarely undertaken." *Id.* at 429 (Alito, J., concurring in the judgment). Therefore, "society'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." *Id.* at 430.

2. These principles dictate that government agents conduct a search when they obtain longer-term historical cell phone location records from a person's cellular service provider.

a. For the same reason that five Justices concluded that there is a reasonable expectation of privacy in longer-term GPS monitoring of a car, there is a reasonable expectation of privacy in longer-term cell phone location records. Any other conclusion would allow the government to circumvent the principle accepted by five Justices in *Jones* through the simple expedient of obtaining cell phone location records. People use their cell phones throughout the day—when they are at home, work, or school, when

they are in the car or on public transportation, when they are shopping or eating, and when they are visiting the doctor, a lawyer, a political associate, or a friend.[5] People even keep their phones nearby and turned on while they are asleep.[6] Indeed, "nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower." *Riley*, 134 S. Ct. at 2490.

"[D]etails about the location of a cell phone can provide an intimate picture of one's daily life." *State v. Earls*, 70 A.3d 630, 642 (N.J. 2013). Historical CSLI "can reveal not just where people go—which doctors, religious services, and stores they visit—but also the people and groups they choose to affiliate with and when they actually do so." *Commonwealth v. Augustine*, 4 N.E. 3d 846, 861 (Mass. 2014) (quoting *Earls*, 70 A.3d at 642). And to state the obvious, when people make a "visit to a gynecologist, a psychiatrist, a bookie, or a priest," they typically "assume that the visit is private." *United States v. Davis*, 754 F.3d 1205, 1216 (11th Cir. 2014) (Sentelle, J.), *rev'd en banc*, 785 F.3d 498 (11th Cir. 2015).

CSLI can also reveal that people are present in their own homes or the homes of their closest friends and relatives, even when that fact is otherwise undiscoverable. Such information gathering "falls

---

[5] Hendrik Müller et al., *Understanding and Comparing Smartphone and Tablet Use: Insights from a Large-Scale Diary Study*, Proceedings of the 27th Australian Computer-Human Interaction Conference 427, 432 (2015), https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/44200.pdf.

[6] *Id.*

within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance" from a public place, such as whether "a particular article is actually located at a particular time in the private residence," or to later confirm that the article remains on the premises. *United States v. Karo*, 468 U.S. 705, 707, 715 (1984).

b. Allowing law enforcement to obtain such records free and clear of any Fourth Amendment restriction would dramatically shrink the amount of privacy that people enjoyed from the time of the Framing through the dawn of the digital age. Prior to the widespread adoption of cell phones, the government simply could not have obtained a comprehensive record of a person's past locations and movements over an extended period. Even "in the context of investigations involving extraordinary offenses," *Jones*, 565 U.S. at 431 (Alito, J., concurring in the judgment), law enforcement agents could have retrieved at best only fragmentary historical location records: perhaps an employee's timecard from the start of a shift, a few scattered store receipts, or a bit of commercial surveillance camera footage. But never could the government have successfully assembled a minute-by-minute transcript of a person's long-concluded movements over days, weeks, or months.

Indeed, prior to the digital age, the only way for the government conceivably to have obtained anything close to an "average of 134 data location points per day," *Graham*, 824 F.3d at 447 (Wynn, J., dissenting in part)—or "one location data point every *five and one half minutes*," *Davis*, 785 F.3d at 540 (Martin, J., dissenting)—would have been to ask the

suspect to recall his past movements and divulge them to police. But that exercise would be severely limited by the vagaries of human memory and the Fifth Amendment's privilege against self-incrimination, *see Kastigar v. United States*, 406 U.S. 441, 444-45 (1972).

Accordingly, the power to "reconstruct someone's specific movements down to the minute, not only around town but also within a particular building," *Riley*, 134 S. Ct. at 2490 (citing *Jones,* 565 U.S. at 415 (Sotomayor, J., concurring)), gives police access to "a category of information that *never* would be available through the use of traditional law enforcement tools of investigation." *Augustine*, 4 N.E.3d at 865; *see also Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) (location information obtained through modern technologies triggers the Fourth Amendment because it offers a never-before-available "precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations").

To be sure, the CSLI at issue here involves historical location data, rather than the real-time tracking that GPS devices provide. But this only strengthens the claim for Fourth Amendment protection. Absent constitutional oversight, the availability of CSLI records would make it "relatively easy and cheap," *Jones*, 565 U.S. at 429 (Alito, J., concurring in the judgment), for the government to pervasively track virtually any American. With uninhibited access to cell phone location data, police would not need to surreptitiously attach a GPS tracker to a target's car, nor return periodically to

covertly change the tracker's batteries. *See, e.g.*, *United States v. Sparks*, 711 F.3d 58, 60 (1st Cir. 2013). The risk of the suspect discovering the surveillance would be zero, and a law enforcement agency would be limited neither by the number of agents in its employ nor the number of tracking devices it could afford. For only a nominal fee to the suspect's service provider—or no fee at all—law enforcement could obtain a detailed journal of a person's locations and movements over a very long period.[7] The available data is limited only by the retention policies of service providers, which are typically long: five years for AT&T, 18 months for Sprint, one year for Verizon.[8]

The ready availability of CSLI makes real the Court's concern in *United States v. Knotts* about "dragnet type law enforcement practices" that make possible "twenty-four hour surveillance of any citizen of this country." 460 U.S. 276, 283-84 (1983) (citation omitted). "When requests for cell phone location

---

[7] Letter from William B. Petersen, Gen. Counsel, Verizon Wireless, to Sen. Edward J. Markey 5 (Oct. 3, 2013), https://www.markey.senate.gov/imo/media/doc/2013-12-09_VZ_CarrierResponse.pdf ("In the majority of instances . . . Verizon Wireless does not seek reimbursement for responding to law enforcement requests."); Letter from Charles McKee, Vice President, Sprint Nextel, to Sen. Edward J. Markey 5 (Oct. 3, 2013), http://s3.documentcloud.org/documents/889100/response-sprint.pdf ("Sprint Letter") (charging $30 per hour worked responding to requests for CSLI).

[8] Letter from Timothy P. McKone, Executive Vice President, AT&T, to Sen. Edward J. Markey 3 (Oct. 3, 2013), http://www.markey.senate.gov/imo/media/doc/2013-10-03_ATT_re_Carrier.pdf; Sprint Letter, *supra*, at 2; Silliman, *supra*.

information have become so numerous that the telephone company must develop a self-service website so that law enforcement agents can retrieve user data from the comfort of their desks, we can safely say that 'such dragnet-type law enforcement practices' are already in use." *United States v. Pineda-Moreno*, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing *en banc*).

c. The reasonableness of the expectation of privacy here is bolstered by protections adopted in federal and state law. In assessing whether an expectation of privacy is objectively reasonable, norms and expectations shaped by federal and state statutes are relevant considerations. *See Florida v. Riley*, 488 U.S. 445, 451 (1989) (plurality opinion) (finding that police surveillance from a helicopter did not invade a reasonable expectation of privacy in part because "the helicopter in this case was *not* violating the law" by flying over private property at an elevation of 400 feet).[9]

Federal law protects the confidentiality of cell phone location data by prohibiting cellular service providers from disclosing sensitive customer records—including "information that relates to the . . . location . . . of use of a telecommunications service"—without "approval of the customer." 47 U.S.C. § 222(c)(1), (h)(1)(A). Congress has recognized

[9] Similarly, "[i]n evaluating the reasonableness of police procedures under the Fourth Amendment," this Court has looked to "prevailing rules in individual jurisdictions" and the trend in relevant state laws. *Tennessee v. Garner*, 471 U.S. 1, 15-18 & n.21 (1985) (citing *United States v. Watson*, 423 U.S. 411, 421-22 (1976)).

the particular sensitivity of location information, even beyond the sensitivity of other telecommunications records, by specifying that "a customer shall not be considered to have approved the use or disclosure of or access to . . . call location information" "without [providing] express prior authorization." *Id.* § 222(f). As one of the sponsors of this provision explained, the statute "protects us from Government knowing where you are going and what you are doing in your life." 145 Cong. Rec. H9858–01, at H9860 (daily ed. Oct. 12, 1999) (statement of Rep. Tauzin).[10]

In addition, since 2013 nine states have required law enforcement to obtain a search warrant for historical CSLI by statute or pursuant to judicial interpretation of the state constitution.[11] The high courts of at least seven more states have not yet

---

[10] For assessing reasonable expectations of privacy, the Court looks to the rules governing *public* access to private information or areas, rather than to what law enforcement can do. *See California v. Ciraolo*, 476 U.S. 207, 213-14 (1986); William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 Harv. L. Rev. 1821, 1825-26, 1831 (2016). Thus, the Court in *Ciraolo* looked to whether aerial surveillance by law enforcement took place within legally navigable airspace as determined by federal law, where "[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed." 476 U.S. at 213-14 (citing 49 U.S.C. App. § 1304 (current version at 49 U.S.C. § 40103)).

[11] *Commonwealth v. Augustine*, 4 N.E.3d 846 (Mass. 2014); Cal. Penal Code § 1546.1(b); Me. Rev. Stat. tit. 16, § 648; Minn. Stat. §§ 626A.28(3)(d), 626A.42(2); Mont. Code Ann. § 46-5-110(1)(a); N.H. Rev. Stat. Ann. § 644-A:2; 12 R.I. Gen. Laws § 12-32-2; Utah Code Ann. § 77-23c-102(1)(a); Vt. Stat. Ann. tit. 13, § 8102(b); *see also* Kan. Stat. Ann. § 22-2502(a)(1)(G)(i).

addressed CSLI specifically but have recognized a reasonable expectation of privacy in telephone dialing or billing records more generally.[12] Additional states explicitly require a warrant for real-time cell phone location data.[13] In combination, these laws reflect "public attitudes" toward the expectation of privacy in cell phone location records, *see Jones*, 565 U.S. at 429 (Alito, J., concurring in the judgment), and make it reasonable for individuals to expect that their everyday location and movements over an extended period will remain private.

These laws also support a normative judgment that the privacy of this information is integral to living in a free and democratic society. As the Court noted in *Smith v. Maryland*, 442 U.S. at 740 n.5, the reasonable-expectation-of-privacy inquiry includes a normative component, in order to avoid significant erosion of privacy protections central to our constitutional order. Allowing the government to freely obtain the detailed whereabouts of any—or all—of its citizens without a warrant would dramatically "alter the relationship between citizen and government in a way that is inimical to democratic society," *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

---

[12] *See* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 Cath. U. L. Rev. 373, 396-99 & nn.118-28 (2006) (citing cases from the high courts of, *inter alia*, Colorado, Hawaii, Idaho, Illinois, New Jersey, Pennsylvania, and Washington).

[13] *See Tracey v. State*, 152 So. 3d 504 (Fla. 2014); *State v. Earls*, 70 A.3d 630 (N.J. 2013); 725 Ill. Comp. Stat. 168/10; Ind. Code § 35-33-5-12; Md. Code Ann. Crim. Proc. § 1-203.1(b).

3. Contrary to the Sixth Circuit's reasoning, Pet. App. 14a-15a, acquisition of CSLI intrudes on reasonable expectations of privacy even if CSLI data is sometimes less precise than GPS data. Any attempt to differentiate between CSLI and GPS information is unsupportable in fact, not administrable in practice, and likely to become obsolete as technology advances.

a. While the CSLI in this case, which reflects the state of the technology in 2010 and 2011, did not generally yield GPS-level precision, it was nonetheless highly revealing. Petitioner's cellular service provider recorded and retained information about the location of petitioner's phone at the start and end of both outgoing and incoming calls. Pet. App. 4a. Each location point in the records identified the wedge-shaped cell site sector in which the phone was located at a particular time. The size of those sectors varied widely. In a sparsely populated rural area, a cell site's coverage area might have extended for miles. Pet. App. 5a. In a dense urban or suburban area, cell sites were (and continue to be) located much closer together—down to a few hundred meters apart or, in the case of small cells, significantly less. Hoy, *supra*, at 69-70, 244.

Accordingly, the prosecution used petitioner's CSLI to demonstrate that he was "right where the first robbery was at the exact time of the robbery, the exact sector," J.A. 131, and that he was "right in the right sector before the Radio Shack in Highland Park," J.A. 132. The prosecution also argued that petitioner's phone was in a location on December 13, 2010, "consistent with the geographic area that encompasses the robbery scene," J.A. 58, and that his

location data provided "corroboration" to other evidence in the case, J.A. 131.

b. Even comparatively less precise location information can enable law enforcement to infer the exact location of a phone inside a home or other building. For example, "the 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." *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* (*Third Circuit CSLI Opinion*), 620 F.3d 304, 311-12 (3d Cir. 2010); *accord Davis*, 785 F.3d at 540-41 (Martin, J., dissenting) (same). The government has used CSLI to place defendants "literally right up against the America Gas Station immediately preceding and after [the] robbery occurred," *Davis*, 785 F.3d at 541 (Martin, J., dissenting) (alteration in original) (quoting trial transcript), "literally . . . right next door to the Walgreen's just before and just after that store was robbed," *id.* (alteration in original), and "right close to the McDonalds" before the robbery of that business, Trial Tr. of Apr. 27, 2012 at 96, *United States v. Graham*, 846 F. Supp. 2d 384 (D. Md. 2012) (No. RDB-11-0094), *aff'd* 824 F.3d 421 (4th Cir. 2016), *petition for cert. filed*, No. 16-6308.

CSLI reveals not just where a person was at discrete moments, but where she was going. In this case, the government presented testimony explaining that cell site data points revealed petitioner's trajectories placing him at certain businesses at the relevant times. *See* J.A. 59, 61-62, 66-67; *see also United States v. Stimler*, __ F.3d __, 2017 WL

3080866, at *16 (3d Cir. July 7, 2017) (Restrepo, J., concurring in part) ("The [government] expert also used CSLI to describe an individual's 'southbound movement on I-278.'"). And CSLI even allows the government to learn with whom a person associated and when, by matching the location information of two or more individuals. *See, e.g.*, Pet. App. 81a-82a (concluding that petitioner and his co-defendant were at the same location based on their CSLI records); J.A. 133 (same).

Finally, cell site location information can "identify various patterns of life"[14] and "identify important places in people's lives" such as their home and work.[15] When paired with other information about phone calls and text messages stored by service providers, it can even facilitate prediction of a cell phone user's personality traits.[16]

c. Regardless of the precise granularity of the technology used in this case, "the rule [the Court]

---

[14] Neal Walfield et al., *A Quantitative Analysis of Cell Tower Trace Data for Understanding Human Mobility and Mobile Networks*, 6th International Workshop on Mobile Entity Localization, Tracking and Analysis 8 (Oct. 10, 2016), https://hal.inria.fr/hal-01378622/document.

[15] Sibren Isaacman et al., *Identifying Important Places in People's Lives from Cellular Network Data*, Proc. of 9th International Conference on Pervasive Computing 2 (June 2011), http://kiskeya.org/ramon/work/pubs/pervasive11.pdf.

[16] Rodrigo de Oliveira et al., *Towards a Psychographic User Model from Mobile Phone Usage*, Proceedings of the ACM CHI 2011 Conference on Human Factors in Computing Systems 2195 (2011), http://www.ic.unicamp.br/~oliveira/doc/CHI2011-WIP_Towards-a-psychographic-user-model-from-mobile-phone-usage.pdf.

adopt[s] must take account of more sophisticated systems that are already in use or in development." *Kyllo*, 533 U.S. at 36. And today, "the proliferation of . . . cell towers has resulted in smaller coverage areas and CSLI that is far more accurate—in some cases as good as GPS." *Stimler*, 2017 WL 3080866, at *17 (Restrepo, J., concurring in part) (internal quotation marks and citation omitted). As one expert in cellular infrastructure has explained, "the precision of [CSLI] data will vary widely for any given customer over the course of a given day, from the relatively less precise to the relatively very precise . . . . For a typical user, over time, some of that data will inevitably reveal locational precision approaching that of GPS."[17]

Cellular service providers can now calculate the "approximate distance the [cell phone] is from the cell site," instead of just logging which sector it is in. Silliman, *supra*. In addition, providers are increasing their network coverage by deploying low-power "small cells," sometimes called "microcells," "picocells," and "femtocells," which provide service to much smaller areas than traditional cell sites. Hoy, *supra*, at 69-70; *Graham*, 824 F.3d at 448 (Wynn, J., dissenting). The number of small cells in the United States now exceeds the number of traditional cell

[17] *The Electronic Communications Privacy Act (ECPA), Part 2: Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism & Homeland Sec. of the H. Comm. on the Judiciary*, 113th Cong. 15 (2013) (statement of Matt Blaze, Associate Professor, University of Pennsylvania), https://judiciary.house.gov/wp-content/uploads/2016/02/Blaze-Testimony.pdf.

sites.[18] Callers connecting to a carrier's small cells can be located to a high degree of precision, "such as one floor of a building, the waiting room of an office, or a single home." *Graham*, 824 F.3d at 448 (Wynn, J., dissenting).[19]

CSLI is also becoming more voluminous. Cellular service providers now collect and retain location information not just for the start and end of calls, but for text messages and data connections, "such as checking email, watching a video, or using apps." Silliman, *supra*; *see also* Hoy, *supra*, at 255. During internet-based data connections, service providers "collect[] multiple location points." Silliman, *supra*. Americans "spend two hours and 32 minutes a day[,] on average, using apps or accessing the web on their smartphones—a figure that has doubled in the past year alone." CTIA, *Wireless Snapshot 2017*, at 4 (2017).[20] Even when people are not actively using their phones, many email and social media apps regularly contact the network to

---

[18] *Compare* Michael Carroll, *Small Cells Hit Milestone*, FierceWireless, Nov. 1, 2012, http://www.fiercewireless.com/europe/small-cells-hit-milestone (noting Sprint's deployment of one million femtocells in the United States as of 2012), *with* CTIA, *Annual Wireless Industry Survey* (2017), *supra*, at 5 (301,779 traditional cell sites erected by all U.S. cellular carriers as of 2012).

[19] Wireless providers are able to identify the location of small cells in order to comply with emergency calling location requirements (E-911). *See* Fourth Report & Order 18 & n.94, *In re Wireless E911 Location Accuracy Requirements*, PS Docket No. 07-114 (F.C.C. Jan. 29, 2015), https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-9A1.pdf.

[20] https://www.ctia.org/docs/default-source/default-document-library/ctia-wireless-snapshot.pdf.

check for new messages, thus generating a steady stream of location data that would easily eclipse the 101 location points per day represented in petitioner's records. *See* 6th Cir. Doc. No. 29, at 9. This trend toward greater precision and more comprehensive tracking is sure to continue.

Thus, a rule that protects GPS data but not CSLI is doomed to obsolescence and would render the protection established in *Jones* a dead letter. The GPS data at issue in *Jones* itself lacked pinpoint precision, establishing the vehicle's location within only 50 to 100 feet. *Jones*, 565 U.S. at 403. Some CSLI data points already approach this level of precision, and the precision of CSLI will only increase. Indeed, service providers are already able to precisely locate phones in real time by triangulating their location based on signals received from multiple nearby towers. *See In re Application of the U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F. Supp. 2d 526, 532-34 (D. Md. 2011).[21]

4. Because "the duration of the period for which historical CSLI is sought will be a relevant consideration in the reasonable expectation of

[21] When the government requests historical CSLI it has no way to know in advance how many data points will be for small cells or geographically small sectors, or will otherwise reveal especially precise location information. Nor will it know how frequently a suspect uses his phone, and thus what volume of location data is available. As this Court observed in *Kyllo*, "[n]o police officer would be able to know in advance whether his through-the-wall surveillance picks up 'intimate' details—and thus would be unable to know in advance whether it is constitutional." 533 U.S. at 39. Only clear guidance from this Court will provide adequate constitutional protection.

privacy calculus," there is "some period of time for which the [government] may obtain a person's historical CSLI [free from Fourth Amendment scrutiny], because the duration is too brief to implicate the person's reasonable privacy interest." *Augustine*, 4 N.E.3d at 865; *see also Jones*, 565 U.S. at 430 (Alito, J., concurring in the judgment). As in *Jones*, however, the Court "need not identify with precision the point at which" the duration of CSLI constitutes a search. "[T]he line was surely crossed" in this case well before the 127-day mark. *Jones*, 565 U.S. at 430 (Alito, J., concurring in the judgment); *see also United States v. Place*, 462 U.S. 696, 709-10 (1983) (holding that the seizure and detention of a traveler's luggage was too lengthy to qualify as "brief" under *Terry v. Ohio*, 392 U.S. 1 (1968), but declining to set a precise time limit for such detentions).

When the time comes to provide precise guidance to law enforcement agents and lower courts, this Court will have ample authority to do so. Across several realms of constitutional criminal procedure, the Court has not hesitated to set bright-line durational limits in order to "provide some degree of certainty [to law enforcement that its conduct] . . . fall[s] within constitutional bounds." *Cty. of Riverside v. McLaughlin*, 500 U.S. 44, 56 (1991) (requiring a judicial determination of probable cause within 48 hours of arrest); *see also, e.g.*, *Maryland v. Shatzer*, 559 U.S. 98, 110 (2010) (holding that once a suspect has invoked his right to counsel, police may not restart custodial questioning for 14 days); *Baldwin v. New York*, 399 U.S. 66, 69 (1970) (holding that the right to a jury trial is triggered whenever the charged offense is punishable

by more than six months' confinement). In the context of historical CSLI, the durational limit should recognize that police would previously have been able to obtain a small quantity of historical location information by canvassing witnesses and collecting other evidence near the scene of a crime, but never could have compiled a minute-by-minute accounting of a suspect's locations over days, weeks, or longer. Drawing a line that protects against collection of longer-term location records is crucial to preserving the privacy that Americans enjoyed from the Framing to the dawn of the digital age.[22]

---

[22] It is also critical to ensure that the line between short term and long term in the context of CSLI does not provide law enforcement a means of evading the durational protection that *Jones* establishes. *Jones*, 565 U.S. at 429-30 (Alito, J., concurring in the judgment). Lower courts applying *Jones* to real-time cell phone location tracking have concluded that tracking for periods ranging from seven hours to four days does not constitute longer-term surveillance under the Fourth Amendment. *See United States v. Riley*, 858 F.3d 1012, 1018 (6th Cir. 2017) (seven hours); *United States v. Wigginton*, No. 6:15-CR-5-GFVT-HAI-1, 2015 WL 8492457, at *4 (E.D. Ky. Dec. 10, 2015) (24 hours); *United States v. Skinner*, 690 F.3d 772, 780 (6th Cir. 2012) (three days); *Ford v. State*, 477 S.W.3d 321, 334-35 (Tex. Crim. App. 2015) (four days). *But see Tracey v. State*, 152 So. 3d 504, 520 (Fla. 2014) (real-time cell phone location tracking is a search, regardless of duration). Only one court has drawn a line in the context of historical cell site location records, and it has concluded (as a matter of state constitutional law) that anything more than six hours is long term and therefore a search. *Commonwealth v. Estabrook*, 38 N.E.3d 231, 237 (Mass. 2015).

B. Law Enforcement Access To Cell Site Location Information Interferes With The Security Of A Person's Private "Papers."

A property-based analysis under the Fourth Amendment provides an independent ground for holding that the government conducts a search (or seizure) when it obtains a person's CSLI.

As this Court made clear in *Jones*, "the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*," property-based conceptions of Fourth Amendment rights. *Jones*, 565 U.S. at 409; *see also Florida v. Jardines*, 133 S. Ct. 1409, 1415-16 (2013). Thus, a search necessarily occurs whenever the government intrudes without consent on a person's "papers" or "effects" through trespass or seizure for purposes of gathering information. *See Jones*, 565 U.S. at 406 (citing U.S. Const. amend. IV).

Determining whether the government has interfered with the security of papers or effects within the meaning of the Fourth Amendment requires reference to some external source of law that defines a person's right to exclude others from those papers or effects—be it common-law trespass and property principles, *id.* at 404-05 & n.2, or positive law, *see* William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 Harv. L. Rev. 1821 (2016); Richard M. Re, *The Positive Law Floor*, 129 Harv. L. Rev. F. 313 (2016). Where a source of law protects against access by the *public* without consent, the Fourth Amendment protects against unreasonable access by the *government* as well. Baude & Stern, 129 Harv. L.

Rev. at 1825-26. That is why this Court concluded in *Jardines* that because members of the public lack an implied license under common-law principles to enter and remain on a home's curtilage with a drug-sniffing dog, police officers implicate the Fourth Amendment when engaging in that same conduct. 133 S. Ct. at 1415-16.

Here, the federal Telecommunications Act designates cell phone location information as "customer proprietary network information" ("CPNI")—a category of records that the service provider cannot disclose absent "approval of the customer." 47 U.S.C. § 222(c)(1)-(2), (h)(1)(A). As the Federal Communications Commission explains, location information "clearly qualifies as CPNI," and therefore subjects service providers to "a duty to protect [its] confidentiality." *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 28 FCC Rcd. 9609, 9616, 9619 ¶¶ 22, 29 (2013).

Originally enacted in 1996, the CPNI provision was amended in 1999 to explicitly protect cell phone location information by prohibiting service providers from using or disclosing it "without the express prior authorization of the customer." 47 U.S.C. § 222(f); *see also* Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, § 5, 113 Stat. 1286, 1288. The statute provides a mechanism for people to enforce their right to protect their location information against dissemination without consent, in the form of a civil remedy against service providers. 47 U.S.C. § 207. Congress erected yet more

protections for cell phone location data in 2007 when it made it a crime for any person to obtain or attempt to obtain that information by fraudulent means. 18 U.S.C. § 1039(a), (h)(1)(A); *see also* Telephone Records and Privacy Protection Act of 2006, Pub. L. No. 109-476, § 3(a), 120 Stat. 3568, 3569. Thus, as cell phone technology has become more advanced and more widely adopted, Congress has increasingly legislated safeguards against nonconsensual dissemination of CSLI.

The proprietary interest created by statute makes clear that CSLI is the "paper" or "effect" of the customer. "[T]o the extent CPNI is property, . . . it is better understood as belonging to the customer, not the carrier."[23] By restricting the use and transfer of CSLI without consent of the customer, the Telecommunications Act grants that customer a right to exclude others from it. As required by federal regulations, service providers take concrete steps to guarantee that right: During petitioner's time as a MetroPCS customer, for example, that company would release a subscriber's CPNI only to that subscriber, and only "upon the subscriber's provision of the correct password" over the phone or "presentation of valid identification" during an in-person request. MetroPCS, Annual 47 C.F.R. § 64.2009(e) CPNI Certification, EB Docket 06-036 (Mar. 1, 2011), https://ecfsapi.fcc.gov/file/7021032829.pdf. Accordingly, the government's obtaining of

[23] Second Report & Order and Further Notice of Proposed Rulemaking, *In re Implementation of the Telecommunications Act of 1996*, 13 FCC Rcd. 8061, at *14 (1998), *vacated on other grounds by U.S. West, Inc. v. F.C.C.*, 182 F.3d 1224 (10th Cir. 1999).

personal CSLI information invades individuals' "papers" and "effects," and constitutes a search.

C. Pre-Digital Cases Concerning The Third-Party Doctrine Do Not Govern This Case.

1. Cell Site Location Information Is Far More Sensitive Than the Phone and Bank Records Involved in *Smith* and *Miller*, and Unlike Those Records, Is Not Voluntarily Conveyed.

The Sixth Circuit believed that two cases from the pre-digital age—*Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976)—constituted "binding precedent" precluding application of the Fourth Amendment to the records at issue. Pet. App. 12a-14a; *see also* BIO 14. They do not. There is no basis in this Court's jurisprudence for extending *Smith* and *Miller* to CSLI, both because the information is more sensitive, and because it is not voluntarily shared with a third party in any meaningful way.

In *Smith*, this Court ruled that the use of a pen register for several days to capture the telephone numbers a person dials does not implicate a reasonable expectation of privacy. 442 U.S. at 740-42. The Court assessed the degree of invasiveness of the surveillance to determine whether the caller had a reasonable expectation of privacy, noting the "pen register's limited capabilities" and explaining that "a law enforcement official could not even determine from the use of a pen register whether a communication existed." *Id.* at 741-42 (citation

omitted). The Court emphasized that when dialing a phone number, the caller "voluntarily convey[s] numerical information to the telephone company." *Id.* at 744. People must know this, the Court explained, because they have to "convey" phone numbers to the phone company in the process of dialing them, and because "they see a list of their long-distance (toll) calls on their monthly bills." *Id.* at 742.

Similarly, in *Miller* the Court concluded that a bank customer lacked any Fourth Amendment interest in several months' worth of canceled checks, deposit slips, and account statements held by a bank. 425 U.S. at 438, 440. The Court explained that "[w]e must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents." *Id.* at 442. The Court concluded that there was a low privacy interest in the records, because "[t]he checks are not confidential communications but negotiable instruments to be used in commercial transactions." *Id.* As in *Smith*, the Court also noted that the government obtained "only information voluntarily conveyed to the banks." *Id.*

This Court need not disturb the holdings of *Smith* and *Miller* to conclude that they do not apply in this context. The particular records at issue here are far more sensitive and personal than those in *Smith* and *Miller*, and are not conveyed in a meaningfully voluntary way. Indeed, the typical user is not even aware that the cellular service provider has this compendium of sensitive information.

a. The degree of sensitivity in the information here is alone sufficient to distinguish *Smith* and

Miller. That is the teaching of the concurrences in *Jones*. Before that case, this Court had applied *Smith* to hold that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another" because he "voluntarily convey[s] to anyone who want[s] to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination." *Knotts*, 460 U.S. at 281-82. But in *Jones*, five Justices concluded that longer-term surreptitious GPS monitoring of cars traveling on public streets violates reasonable expectations of privacy. Longer-term GPS information is so personally sensitive and so unlikely to have been obtained in the pre-digital era that it triggers a reasonable expectation of privacy, regardless of whether the locational information it contains was theoretically disclosed to the entire public at large.

Indeed, to assess individuals' expectations of privacy in records or information held by a third party, this Court has *never* relied simply on the fact that they were shared, but has also looked to what privacy interest a person has in the information the records reveal. *See, e.g.*, *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (reasonable expectation of privacy in diagnostic test records held by hospital); *Stoner v. California*, 376 U.S. 483, 485, 489-90 (1964) (Fourth Amendment protects privacy in hotel room even though a guest "undoubtedly gives implied or express permission to such persons as maids, janitors or repairmen to enter his room in the performance of their duties" (internal quotation marks and citation omitted)). Far from being a formalistic rule, the "third party" doctrine is really

just a shorthand for one factor in the overall reasonable-expectation-of-privacy analysis—a factor that can be overcome when highly sensitive information is at stake.

That is the case here. Just as in *Jones* and *Riley*, "any extension of [pre-digital] reasoning to digital data has to rest on its own bottom." *Riley*, 134 S. Ct. at 2489. Here, the 186 pages of cell phone location records covering four months are orders of magnitude more granular and revealing than the records in *Smith* and *Miller*. Equating a comprehensive digital repository of cell phone location records with a few days of dialed telephone numbers or even several months' worth of canceled checks "is like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Riley*, 134 S. Ct. at 2488. Both are records in the possession of a third party, "but little else justifies lumping them together." *Id.*

It is no answer to assert, as the Sixth Circuit did, that CSLI cannot be protected under the Fourth Amendment because it does not reveal "the *content* of personal communications." Pet. App. 9a-11a (emphasis added). Though this Court has "occasionally described" its conclusions in terms of contents of communications, it has "never suggested that this concept can serve as a talismanic solution to every Fourth Amendment problem." *Katz*, 389 U.S. at 351 n.9 (citations omitted). *Jones* illustrates as much: GPS information is nothing more than a record of movements; it does not convey any substantive content of personal communications. And yet five Justices have concluded that the Fourth Amendment protects it under the reasonable-

expectation-of-privacy test. *See also Kyllo*, 533 U.S. at 36 (extending Fourth Amendment protection to use of a thermal imaging camera to observe heat emanating from a house, even though an inferential step is required to deduce sensitive information about the interior of the home).

b. *Smith* and *Miller* also do not control because there is no meaningfully voluntary conveyance of CSLI. The act of possessing a cell phone, and even more so the transmission of location information, is not voluntary in any meaningful way.

i. The government asserts that any person who "cho[o]se[s] to carry a cell phone" "takes the risk" that her service provider will reveal days, weeks, or months of her location information to the government. BIO 16. Under this theory, the "choice" that exposes a person's location history to warrantless search is not the knowing placement of a call or sending of a text message, but any possession of a cell phone. Location information is generated not only for outgoing communications initiated by the phone user, but also for *incoming* calls (whether answered or not) and text messages, and for countless data connections made without any active participation of the user, such as when a phone sitting in a person's pocket or purse checks every few seconds or minutes for new emails or social media updates.

The mere act of possessing a cell phone does not voluntarily disclose a comprehensive record of one's movements in any meaningful sense. Modern cell phones are "a pervasive and insistent part of daily life." *Riley*, 134 S. Ct. at 2484. Virtually every American adult has a cell phone, and people feel

compelled to carry their cell phones with them nearly everywhere they go, serving as "necessary instruments for self-expression, even self-identification." *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010). Many employers also demand that people remain digitally "in touch" at all times—or at least when away from the office during normal business hours.

Alternative means of enabling this type of communication are fast disappearing—or never existed in the first place. A majority of American homes now do not have a landline telephone, as residents rely exclusively on cell phones.[24] The number of pay phones in the United States has plummeted from more than two million in 1997, to less than 100,000 today.[25] And no other device—past or present—allows people to text, email, check social media, and follow daily political announcements while away from home or the office. In short, smartphones are "not just another technological convenience"; they have become indispensable for full participation in family, social, professional, civic, and political life. *Riley*, 134 S. Ct. at 2494.

Furthermore, cell phones are now vital instruments of personal safety. For many, they are

---

[24] Stephen J. Blumberg & Julian V. Luke, Ctrs. for Disease Control & Prevention, Nat'l Ctr. for Health Statistics, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, July–December 2016* 1 (2017), https://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201705.pdf.

[25] F.C.C., Indus. Analysis & Tech. Div., *Payphone Data from 1997 Through 2016* tbl.1 (2017), https://www.fcc.gov/file/12198/download.

the exclusive means to call first responders, physicians, or family members in a medical emergency or to report a crime; to seek roadside assistance or summon police after a car accident, flat tire, or vehicle breakdown; to get directions when lost; and to check on the whereabouts of a child. "[A]bout 70 percent of 911 calls are placed from wireless phones, and that percentage is growing. For many Americans, the ability to call 911 for help in an emergency is one of the main reasons they own a wireless phone." F.C.C., *911 Wireless Services*.[26] Ready access to a functioning cell phone provides a level of security that most Americans cannot realistically give up.

Finally, smartphones are fast gaining capacity to be used as critical medical instruments. New software allows them to monitor bodily functions and transmit data to doctors in real time. Eric J. Topol, *The Future of Medicine Is in Your Smartphone*, Wall St. J., Jan. 9, 2015.[27] If a person's doctor instructs her to carry a smartphone to monitor her heart rate or the amount of a certain chemical in her bloodstream, following that instruction can hardly be considered a "voluntary" act that assumes the risk that the government might track the person's every movement. The same is true of an equivalent request

---

[26] https://www.fcc.gov/consumers/guides/911-wireless-services. *See also* Pew Research Ctr., *U.S. Smartphone Use in 2015* 25 (2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015 ("Fully 53% of smartphone owners indicate that they have been in an emergency situation where having their phone available helped resolve the situation.").

[27] https://www.wsj.com/articles/the-future-of-medicine-is-in-your-smartphone-1420828632.

from one's employer that one remain in touch and available while away from the office. People should not be forced to choose between their privacy and their safety, health, or livelihood.

This is especially so because each of a smartphone's essential functions—calling, texting, emailing, data access, navigation, medical monitoring, and so on—is impossible to use without leaving a trail of location records held by the service provider. There is no way to avoid the aggregation and retention of this location information short of turning off or disabling the phone.

Most smartphones have a location privacy setting that, when enabled, prevents applications ("apps")—such as a GPS navigation app—from accessing the phone's location. *See, e.g.*, Apple, *iPhone User Guide: Location Services*.[28] Users might well believe that enabling this function protects their locational privacy. But this setting has no impact at all upon cellular service providers' ability to log and retain the phone's location. Maxwell Payne, *How to Turn Off GPS on a Cell Phone*, USA Today.[29] Virtually any use of the phone generates a location record. There is no option to close the proverbial phone booth door. *See Katz*, 389 U.S. at 352.

ii. Even if the *possession* of cell phones could be said to be voluntary, the *conveyance of location information* of the type obtained by the government here surely cannot. Though some people may have a

[28] https://help.apple.com/iphone/10/#/iph3dd5f9be.

[29] http://traveltips.usatoday.com/turn-off-gps-cell-phone-21147.html.

general sense that their cell phones must communicate with the service provider's cell towers in order to place and receive calls, they cannot know whether the service provider is logging and retaining that data and in what form or detail: single-tower data or triangulated position; sector information or estimated distance from the nearest cell site. People do not know which cell tower and sector their phone is connected to at any time, how large the coverage area of that tower is, or how long the carrier retains location records. Nor will they know whether their phone was roaming on another carrier's network, as was petitioner's here, Pet. App. 72a, and thus whether a company with which they have no contractual relationship whatsoever is logging and retaining their location. *In re Application for Tel. Info. Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011, 1028-29 (N.D. Cal. 2015).

It is also telling that, unlike in *Smith* and *Miller*, individuals do not receive their CSLI in their monthly bill. *Compare Smith*, 442 U.S. at 742, *with Graham*, 824 F.3d at 445 (Wynn, J., dissenting in part). Even a customer who *wanted* to learn this information could not do so: service providers refuse to disclose location records to customers who request them. Megha Rajagopalan, *Cellphone Companies Will Share Your Location Data – Just Not With You*, ProPublica, June 26, 2012.[30]

Put another way, people do not knowingly or intentionally convey to their service provider a "virtual current biography," *People v. Blair*, 602 P.2d

[30] https://www.propublica.org/article/cellphone-companies-will-share-your-location-data-just-not-with-you.

738, 745 (Cal. 1979), charting their locations and movements over weeks and months. While people may know in some general sense that they have to be near a cell tower in order to make or receive a call, it would be outlandish to extrapolate from that minimum knowledge the conclusion that people knowingly and voluntarily disclose their every movement to the government. There is a huge difference between the knowing act of using a cell phone to make a discrete communication, and the involuntary and generally unknown process by which thousands of individual location points are aggregated into a digital almanac of a cell phone user's life.

2. Extending *Smith* and *Miller* to CSLI Records Would Remove a Great Volume of Other Similarly Sensitive Digital Records from the Protection of the Fourth Amendment.

Although it may someday be necessary to "reconsider the premise" of the third-party doctrine, *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring), it is not necessary in this case to reassess its continued validity in every possible context. Properly understood, the disclosure of information to a third party is but one factor in determining whether a reasonable expectation of privacy exists. *See supra* Part I.C; *see also State v. Walton*, 324 P.3d 876, 901 (Haw. 2014). And this Court has explained that "[i]t would be foolish" to suggest that such Fourth Amendment analyses should not account for "the advance of technology." *Kyllo*, 533 U.S. at 33-34. These principles are sufficient to resolve this case.

At the same time, were the Court to hold that the mere act of disclosing information to a third-party business is enough to defeat any Fourth Amendment protection, it would not only effect "a significant diminution of privacy," *Riley*, 134 S. Ct. at 2493, but would also throw into question whether a vast array of Americans' most highly sensitive records can be be protected in the 21st century against dragnet access at law enforcement's whim. Indeed, under the government's theory, people would have no reasonable expectation of privacy even in their emails, because the contents of those communications are shared with a third party.

"In our time, unless a person is willing to live 'off the grid,' it is nearly impossible to avoid disclosing the most personal of information to third-party service providers on a constant basis, just to navigate daily life." *Davis*, 785 F.3d at 525 (Rosenbaum, J., concurring). People cannot avoid disclosing "the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers[,]the books, groceries, and medications they purchase to online retailers," *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring), the contents of their emails, text messages, and private social media communications to their electronic communication service providers, their search queries to Google, their GPS coordinates and location history to Apple, Google, and Waze, their intimate photos to Apple or Flickr, and their medical queries to WebMD. *See Davis*, 785 F.3d at 536 (Martin, J., dissenting).

Moreover, with the rapid proliferation of the so-called "internet of things," virtually any appliance

or effect can now be connected to the internet and programmed to transmit information about a person's home, body, or movements to a third-party company's cloud-based server. Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 Cal. L. Rev. 805 (2016). Even detailed information about "exercise, moods, sleep patterns, and food intake," *id.* at 818, reproductive health,[31] and sexual activity[32] is now recorded and retained on servers controlled by a third party. Not even utterances within the walls of a home are exempt.[33]

Under the government's theory, this vast array of information would automatically lose Fourth Amendment protection. The Sixth Circuit tried to erect a barricade against such slippage, holding that persons have a reasonable expectation of privacy in the "contents" of communications, such as emails. *United States v. Warshak*, 631 F.3d 266, 285-88 (6th Cir. 2010). But if the Sixth Circuit and the government are correct that *Smith* and *Miller* "resolve this case" because "'a person has no

---

[31] *See* Moira Weigel, *'Fitbit for Your Period': The Rise of Fertility Tracking*, Guardian, Mar. 23, 2016, https://www.theguardian.com/technology/2016/mar/23/fitbit-for-your-period-the-rise-of-fertility-tracking.

[32] *See* Kashmir Hill, *This Sex Toy Tells the Manufacturer Every Time You Use It*, Fusion, Aug. 9, 2016, *available at* https://web.archive.org/web/20170507193448/https://fusion.kinja.com/this-sex-toy-tells-the-manufacturer-every-time-you-use-1793861000.

[33] *See* Tim Moynihan, *Alexa and Google Home Record What You Say. But What Happens to that Data?*, Wired, Dec. 5, 2016, https://www.wired.com/2016/12/alexa-and-google-record-your-voice.

legitimate expectation of privacy in information he voluntarily turns over to third parties,'" BIO 14-15 (quoting *Smith*, 442 U.S. at 743-44), there is no way to distinguish emails—or any other of the data just described—from CSLI.[34] Surely a world in which people could not treat their email communications as private would be a radical departure from the privacy people have long expected with respect to their letters, phone calls, and now electronic communications.

II. SEARCHING CELL SITE LOCATION INFORMATION IS UNREASONABLE WITHOUT A WARRANT.

Though issued by neutral magistrates, the orders that enabled the government to procure petitioner's CSLI were made upon an assertion of "specific and articulable facts showing that there are reasonable grounds to believe that" the records were "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d); Pet. App. 53a. That showing is well short of the probable cause required for a warrant. As the government explained below, "reasonable grounds is less than probable

---

[34] The government has also analogized CSLI to the records in *Smith* and *Miller* on the ground that CSLI data are "business records" that service providers "create for their own purposes." BIO 14. But as explained *infra* at Part II.B, CSLI does not constitute a "business record" in any traditional sense. In any event, this Court should eschew any rule that would hinge Fourth Amendment protection on whether information constitutes a "business record." That term has no established meaning, and is untethered from the relevant Fourth Amendment inquiry: whether there is a reasonable expectation of privacy or a property interest in the records at issue.

cause. . . . [and] reasonable grounds to believe that something is relevant . . . is . . . another gigantic qualification, [because] what might be relevant to something can be really far afield." J.A. 34. In the government's view, government agents do not even "have to show a crime. We merely have to show there's a criminal investigation of a crime." *Id.* And unlike a warrant, an application under section 2703(d) does not require a sworn affidavit from the investigating officer, but is issued upon the assertions of a prosecutor in an unsworn application.

The government nevertheless advances three reasons why the Court should find its warrantless search reasonable: that Congress's 30-year-old mechanism for obtaining a court order without probable cause deserves deference; that this Court's cases involving subpoenas automatically render warrantless searches of records held by businesses reasonable; and that a balancing of law enforcement interests against the privacy invasion at issue renders the warrant requirement unnecessary. *See* BIO 22-26.

Because the Sixth Circuit concluded that the government's acquisition of petitioner's CSLI was not a Fourth Amendment search, it did not address whether the warrantless search of that information was unreasonable. The Court may therefore wish to resolve only the threshold question of whether there was a search, and allow the court of appeals on remand to address in the first instance whether the search conducted by the government was reasonable. *See Cutter v. Wilkinson*, 544 U.S. 709, 718 n.7 (2005) ("[W]e are a court of review, not of first view."); *cf. Jones*, 565 U.S. at 413.

Should the Court wish, however, to reach the question whether the search was reasonable, it should hold that a warrant is required for law enforcement requests for longer-term CSLI. Where an individual has a reasonable expectation of privacy in an item or location to be searched, the search is "*per se* unreasonable under the Fourth Amendment" unless conducted pursuant to a judicial warrant supported by probable cause. *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (quoting *Katz*, 389 U.S. at 357); *accord Quon*, 560 U.S. at 760; *City of L.A. v. Patel*, 135 S. Ct. 2443, 2452 (2015). Only if one of the "few specifically established and well-delineated exceptions" to the warrant requirement applies may government officials conduct a warrantless search. *Gant*, 556 U.S. at 338 (internal quotation marks omitted). Because no exception applies here, search of longer-term historical CSLI pursuant to an order issued on a showing well short of probable cause and lacking in particularity is unreasonable.

A. Congress Has Not Had An Opportunity To Consider This Problem.

The government suggests, and the Sixth Circuit asserted, that "Congress has specifically legislated" on the question of what type of process should govern law enforcement access to CSLI. Pet. App. 15a; *see also* BIO 24. This assertion is mistaken. When Congress enacted the Stored Communications Act in 1986, it neither intended to address nor even considered CSLI, much less whether obtaining longer-term CSLI should require a warrant. Consequently, no deference to this outdated legislative scheme is warranted with respect to CSLI.

In 1986, less than one half of one percent of Americans had a cell phone.[35] There were a mere 1,531 cell sites in the United States (compared to more than 300,000 today).[36] Congress gave no indication that it was aware of the existence of historical CSLI, not to mention that the data would eventually exist as to nearly every American. *See* S. Rep. No. 99-541 (1986); H.R. Rep. No. 99-647 (1986).

When Congress amended the SCA in 1994 to clarify the standard for issuance of an order under section 2703(d),[37] only nine percent of Americans had cell phones, and cellular networks were still fragmented and rudimentary, with less than 18,000 cell sites across the country.[38] Again, there is no indication that Congress even considered historical CSLI. *See* H.R. Rep. No. 103-827 (1994). Congress simply did not anticipate the contemporary ubiquity of cell phones and the volume and precision of CSLI that would be retained by service providers. The SCA accordingly provides no guidance on the question whether warrantless search of CSLI is reasonable.[39]

---

[35] *See* CTIA, *Background on CTIA's Wireless Industry Survey* 2 (2014), https://www.ctia.org/docs/default-source/default-document-library/ctia_survey_ye_2014_graphics.pdf.

[36] *Id.*; CTIA, *Annual Wireless Industry Survey* (2017), *supra*, at 4.

[37] Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 207, 108 Stat. 4279 (1994).

[38] *See* CTIA, *Background on CTIA's Wireless Industry Survey* (2014), *supra*, at 2.

[39] Because the Stored Communications Act in the meantime provides a mechanism for obtaining a warrant for records held by service providers, *see* 18 U.S.C. § 2703(c)(1)(A), in holding that a warrant is required, the Court need not find the SCA

B. Analogy To This Court's Subpoena Cases Does Not Render The Search Reasonable.

The government asserts that the court orders used to obtain petitioner's CSLI are "constitutionally reasonable, because the SCA provides more substantial privacy protections than an ordinary judicial subpoena" by requiring "specific and articulable facts" showing "relevan[ce] and material[ity] to an ongoing criminal investigation," not just a mere assertion of relevance. BIO 24 (quoting 18 U.S.C. § 2703(d)). However, because petitioner has a reasonable expectation of privacy in the records at issue, the government's reliance on the Court's subpoena cases is misplaced.

This Court has held that the government may use administrative subpoenas to procure certain business records and personal records held by third parties. *See Okla. Press Publ'g Co. v. Walling*, 327 U.S. 186, 209 (1946); *Miller*, 425 U.S. at 442-44; *Couch v. United States*, 409 U.S. 322, 336 (1973); *United States v. Powell*, 379 U.S. 48, 57 (1964); *see generally* Christopher Slobogin, *Subpoenas and Privacy*, 54 DePaul L. Rev. 805, 815-24 (2005). Because they are heavily regulated, businesses have, if anything, a diminished Fourth Amendment privacy interest in their own business records. *See United States v. Morton Salt Co.*, 338 U.S. 632, 651-52 (1950). And the Court has upheld the use of

---

unconstitutional. *See In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 617 (5th Cir. 2013) (Dennis, J., dissenting).

administrative subpoenas to obtain personal records held by third parties where "there exists no legitimate expectation of privacy." *Couch*, 409 U.S. at 336 & n.19; *accord Miller*, 425 U.S. at 442-43.

This Court, however, has never held that an administrative subpoena directed to a third party is sufficient to procure records in which the individual whom the government is investigating has a reasonable expectation of privacy. Such a holding would radically expand the subpoena power. It would also subvert the core functions of the Fourth Amendment's warrant requirement: to govern criminal investigative searches and seizures and check government overzealousness. *Johnson v. United States*, 333 U.S. 10, 14-15 (1948); *Katz*, 389 U.S. at 356.

In the context of highly sensitive records held by third parties, the requirements of probable cause, particularity, and judicial review that accompany a warrant are crucial mechanisms for preventing violations of individuals' Fourth Amendment rights. Warrants guarantee notice and, in lieu of the target's opportunity to seek to quash the government's request, warrants issue only after a neutral magistrate's independent determination of probable cause and particularity. By contrast, the Stored Communications Act allows requests for CSLI without probable cause, and expressly provides that the government "is not required to provide notice to a subscriber or customer" whose records are requested by subpoena or order. 18 U.S.C. § 2703(c)(3). Indeed, in the context of administrative subpoenas for records lacking a reasonable expectation of privacy, this Court has held that the government need not

notify the investigative target. *S.E.C. v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984).[40]

In cases where the investigative target herself holds the records the government seeks, she can protect her rights by asserting privilege under the Fifth Amendment, *United States v. Hubbell*, 530 U.S. 27 (2000), or by obtaining pre-enforcement judicial review to argue that the subpoena seeks information beyond what is truly relevant to the investigation, *see Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 415 (1984). But in the context of subpoenas to third parties, there is no Fifth Amendment privilege against production of incriminating information, *Couch*, 409 U.S. at 336, and the third party will often lack the knowledge and incentive to challenge the relevance of a subpoena or its scope. The protections of a warrant, including particularity and probable cause, provide crucial protection against abuse.

C. A Balancing Of Interests Under The Fourth Amendment Commands That A Warrant Is Required.

The government finally argues that the Court should conduct its own general reasonableness inquiry that balances the degree of intrusion on privacy against the strength of the government's interest. BIO 24-26. But as is usually the case, the warrant requirement itself strikes the appropriate

---

[40] Because this case does not involve use of a grand jury subpoena, the Court need not address whether different rules are appropriate for subpoenas issued by a grand jury. *See United States v. R. Enterprises, Inc.*, 498 U.S. 292, 297, 300 (1991) (explaining that "[t]he grand jury occupies a unique role in our criminal justice system," and must be afforded "wide latitude" in its issuance of subpoenas).

Fourth Amendment balance here. *See Camara v. Municipal Ct.*, 387 U.S. 523, 528-29 (1967).

In any event, even if a more general reasonableness analysis were conducted, the government's need for evidence is no greater than in the broad sweep of other searches for which warrants are required, and the privacy interest is high.

1. The government's interest in obtaining historical CSLI in criminal investigations is indistinguishable from its general interest in gathering evidence to investigate crimes. There is, for example, no interest in officer safety, *United States v. Robinson*, 414 U.S. 218, 234 (1973), or accurate identification of arrestees, *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013), that requires jettisoning the warrant requirement. Rather, in this case the government was seeking evidence to inculpate petitioner and eventually convict him at trial. In such cases, this Court has explained that "the warrant requirement is 'an important working part of our machinery of government,' not merely 'an inconvenience to be somehow "weighed" against the claims of police efficiency.'" *Riley*, 134 S. Ct. at 2493 (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 481 (1971)).

Indeed, many law enforcement agencies *already* obtain warrants for CSLI as a matter of state law or local policy. In California, Maine, Massachusetts, Minnesota, Montana, New Hampshire, Rhode Island, Utah, and Vermont, state law mandates use of a warrant for historical CSLI. *See supra* note 11. Elsewhere, a number of police departments—including in the County of Hawai'i and City of Honolulu, Hawai'i; Wichita, Kansas;

Lexington, Kentucky; Lincoln, Nebraska; and North Las Vegas, Nevada—have long required a warrant for historical CSLI as a matter of policy. Am. Civil Liberties Union, *ACLU Affiliate Nationwide Cell Phone Tracking Public Records Requests: Findings and Analysis* 3 (2013).[41] Law enforcement agencies in other states are required to get a warrant for real-time cell-phone location data, *see supra* note 13, as are federal authorities in most of the country, *see United States v. Espudo*, 954 F. Supp. 2d 1029, 1035 (S.D. Cal. 2013).

As the practice in these jurisdictions suggests, the warrant requirement is not unduly burdensome in this context. In the words of the California State Sheriffs' Association when explaining its non-opposition to a bill that codified a warrant requirement for historical CSLI in California, a warrant requirement "ensure[s] that the correct balance is struck between the need for law enforcement to obtain information regarding criminal activities from electronic communications and the privacy interests of those who use email and other forms of electronic communication."[42] Since

---

[41] https://www.aclu.org/sites/default/files/field_document/cell_phone_tracking_documents_-_final.pdf.

[42] Letter from Aaron Maguire, Legislative Counsel, Cal. State Sheriff's Ass'n, to Hon. Mark Leno, Cal. State Senate (Aug. 26, 2015), https://www.eff.org/document/california-state-sheriffs-association-remove-opposition-sb-178-calecpa; *see also* Letter from David Bejarano, President, Cal. Police Chiefs Ass'n, Inc., to Hon. Mark Leno, Cal. State Senate (Aug. 24, 2015), https://www.eff.org/files/2015/09/01/califoria_police_chiefs_association_-_sb_178_leno_-_remove_opposition.pdf (bill does not "imped[e] on law enforcement's ability to serve the needs of their communities").

passage of California's law, law enforcement agencies throughout the state have continued to obtain CSLI pursuant to the newly codified warrant standard. *See* Cal. Dep't of Justice, Office of the Attorney Gen., *Electronic Search Warrant Notifications*, *available at* https://openjustice.doj.ca.gov/data (providing data about subset of warrants issued in first quarter of 2017 for cell phone location information).

2. On the other side of the ledger, the privacy interests are high. As detailed above, longer-term CSLI can reveal a great deal of detailed private information. The orders here, for example, are entirely lacking in particularity and sweep in large quantities of sensitive information without adequate cause. In an attempt to place petitioner at the scenes of eight discrete robberies at known times on eight individual days, the government requested five months and obtained four months (127 days) of petitioner's location data comprising thousands of location data points. Pet. App. 7a, 52a. For the vast majority of those days, the government patently lacked probable cause to believe that a crime had even been committed, much less that petitioner was involved in its commission.

A request for months of data is no aberration: according to T-Mobile, which now owns petitioner's service provider, MetroPCS, the average law enforcement request "asks for approximately fifty-five days of records."[43] Other recent cases involve comparable or even greater quantities of data. In one

[43] T-Mobile, *Transparency Report for 2013 & 2014*, at 5 (2015), http://newsroom.t-mobile.com/content/1020/files/NewTransparencyReport.pdf.

case, in the course of investigating robberies on six days, the government obtained 221 days (more than seven months) of cell site location information, revealing 29,659 location points for one defendant. *Graham*, 824 F.3d at 446-47 (Wynn, J., dissenting in part). Other cases in the courts of appeals have involved government searches of CSLI covering 67 days, *Davis*, 785 F.3d at 501, 57 days, *Stimler*, 2017 WL 3080866, at *2, and 37 days, *United States v. Williams*, 161 F. Supp. 3d. 846, 849 (N.D. Cal. 2016), *appeal pending sub nom. United States v. Gilton*, No. 16-10109 (9th Cir.).

Acquisition of these durations and volumes of CSLI seriously infringes on personal privacy. "[T]he Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley*, 134 S. Ct. at 2494. "The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." *Stanford v. Texas*, 379 U.S. 476, 485 (1965) (citation omitted).

In sum, clarifying that a warrant is required will ensure that law enforcement officers can acquire particular spans of location records where there is probable cause that they will provide evidence of criminal conduct. And it will protect records that are not pertinent to the investigation but that can reveal much private information about a person's life. This

Court should provide a "simple" answer to the question presented: "get a warrant." *Riley*, 134 S. Ct. at 2495.

CONCLUSION

For the foregoing reasons, the judgment of the Sixth Circuit should be reversed.

Respectfully submitted,

Nathan Freed Wessler
Ben Wizner
Brett Max Kaufman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
New York, NY 10004

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

Cecillia D. Wang
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111

Harold Gurewitz
Counsel of Record
GUREWITZ & RABEN, PLC
333 W. Fort Street,
Suite 1400
Detroit, MI 48226
(313) 628-4733
hgurewitz@grplc.com

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

Jeffrey L. Fisher
STANFORD LAW SCHOOL SUPREME COURT LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305

Dated: August 7, 2017