No. 16-402

In the Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

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

BRIEF OF THE CENTER FOR DEMOCRACY AND TECHNOLOGY AS *AMICUS CURIAE* IN SUPPORT OF PETITIONER

ANDREW J. PINCUS
Counsel of Record
Mayer Brown LLP
1999 K Street, NW
Washington, DC 20006
(202) 263-3000
apincus@mayerbrown.com

Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF CONTENTS—continued

Page

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES—continued

Page(s)

Statutes, Rules and Regulations

TABLE OF AUTHORITIES—continued

Page(s)

Other Authorities

TABLE OF AUTHORITIES—continued

Page(s)

TABLE OF AUTHORITIES—continued

Page(s)

TABLE OF AUTHORITIES—continued

Page(s)

TABLE OF AUTHORITIES—continued

Page(s)

TABLE OF AUTHORITIES—continued

Page(s)

TABLE OF AUTHORITIES—continued

Page(s)

INTEREST OF THE *AMICUS CURIAE*

The Center for Democracy & Technology (CDT) is a non-profit, public interest organization focused on privacy and other civil liberties issues affecting the Internet, other communications networks, and associated technologies. CDT represents the public's interest in an open Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

CDT has participated as *amicus curiae* in cases before this Court involving the application of the Fourth Amendment to new technologies, including *Riley* v. *California*, 134 S. Ct. 2473 (2014); *United States* v. *Jones*, 565 U.S. 400 (2012); and *City of Ontario* v. *Quon*, 560 U.S. 746 (2010).[1]

INTRODUCTION AND SUMMARY OF ARGUMENT

This case—like *Riley* v. *California*, 134 S. Ct. 2473 (2014) and *United States* v. *Jones*, 565 U.S. 400 (2012)—brings before the Court an important question regarding the application of the Fourth Amendment in light of the changes wrought by digital technology.

In the pre-digital era, Americans typically stored their personal information at home. Letters, photographs, important documents, health and financial

---

[1] Pursuant to Rule 37.6, *amicus* affirms that no counsel for a party authored this brief in whole or in part and that no person other than *amicus* and its counsel made a monetary contribution to its preparation or submission. The parties' blanket consents to the filing of *amicus* briefs have been filed with the Clerk's office.

information all were printed on paper, which imposed a physical limit on the amount of material that individuals could retain.

Digital technology has transformed the ways that Americans retain their personal information, and also has dramatically altered the quantity and types of personal information that is preserved.

Written letters have largely been replaced by email; and physical documents, photographs, and other records by digital files embodying the same information. This digital data may be stored on an individual's cell phone or laptop computer, but a copy also is likely to be stored "in the cloud" with a third-party service provider.

In addition, third-party service providers collect and retain personal information relating to their customers in the course of providing services to those customers. The cell location information at issue in this case is one example of such information. In addition, fitness and health providers collect and retain detailed information about a customer's physical condition; and Internet browsers retain a record of the websites and individual visits—and that information is accessible by the individual's service provider.

Prior to the widespread adoption of digital technology, this information did not exist because there was no way to gather and preserve it. There was no record of every newspaper, periodical and book that an individual read; or of every location an individual visited; or of a person's minute-by-minute physical condition. Thus, "[i]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical," because govern-

ment officers "would not—and indeed, in the main, simply could not" collect this detailed personal information. *Jones*, 565 U.S. at 429, 430 (Alito, J., concurring in the judgment).

Just as the *Riley* Court took account of the changes wrought by digital technology in applying the search-incident-to-arrest doctrine, the Court in this case must take account of these realities in determining how the Fourth Amendment protects the privacy of highly sensitive personal information in the hands of third parties.

The government argues, and the court below held, that this Court's decisions in *Smith* v. *Maryland*, 442 U.S. 735 (1979), and *United States* v. *Miller*, 425 U.S. 435 (1976), stand for the proposition that personal information in the hands of a third party is not protected by the Fourth Amendment. But neither *Smith* nor *Miller* rested exclusively on the third party's possession of the information—in both cases the Court also discussed the nature of the information at issue.

More fundamentally, there is a vast difference between the narrow types of personal information addressed in *Smith* and *Miller* and the myriad categories and huge amounts of personal information that third parties hold today. For that reason, "any extension of [those cases'] reasoning to digital data has to rest on its own bottom." *Riley*, 134 S. Ct. at 2489.

The changes resulting from digital technology—with Americans storing vast quantities of personal information with third parties, and third parties creating databases of personal information not previously available—make it eminently reasonable to

conclude that Americans have a legitimate expectation of privacy with respect to much of this information. Indeed, holding generally that the Fourth Amendment does not protect an individual's personal information whenever that information is possessed by a third party would—because of these changes—dramatically reduce the protection provided by the Fourth Amendment.

For these reasons, the Court should conclude that the mere fact that personal information is possessed by a third party does not preclude a determination that individuals have an expectation of privacy with respect to that information "that society is prepared to recognize as 'reasonable.'" *Katz* v. *United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

The Court also should recognize that whether the individual provided personal information "voluntarily" should not be accorded any weight in the reasonable-expectation-of-privacy inquiry, because there is no correlation between the voluntary provision of information to a third party and legitimate expectations of privacy. For example, individuals voluntarily transfer the contents of emails, photographs, and sensitive personal documents to third-party service providers who store this information. Yet individuals believe, correctly, that absent very unusual circumstances, this information will be private: it will not be viewed by anyone other than themselves or persons who they authorize. If voluntary provision of information alone precluded Fourth Amendment protection, this highly private information could be obtained by the government without a warrant.

There is a reasonable expectation of privacy in the 127 days of cell site location data at issue here.

Providing a cell phone's location is the equivalent of describing its owner's movements, which is information—like the GPS tracking in *Jones*—that would have been private because the government would not have been able to compile it in the pre-digital era.

Moreover, location information can be combined with other information available to the government to learn about the private aspects of a person's life. Comparing the routes and locations visited by an individual with databases listing the residents, businesses, and other organizations located in those places can reveal religious or political affiliations and other sensitive personal attributes.

The fact that cell phone location data may sometimes be less precise than GPS tracking does not warrant a different result. The relevant comparison is to the information available to the government before the advent of digital technology, and cell location information is dramatically more precise than any tracking that the government would have been able to undertake. In addition, a constitutional rule based on the particular level of precision of the cell phone location information at issue in each case would be wholly impractical. Officers could not know in advance how accurate the information would be and therefore could not anticipate whether a warrant would be required. And courts would face very difficult line-drawing issues.

The circumstances under which third parties acquire and retain cell location data provide further support for a reasonable expectation of privacy. Creation of this data is an unavoidable consequence of using a cell phone, which is a necessity of life in today's world. And a cell service provider's dissemination of this information is strictly limited by federal

and state law. Those facts further enhance the reasonable expectation of privacy.

ARGUMENT

THE FOURTH AMENDMENT'S WARRANT REQUIREMENT APPLIES TO THE CELL PHONE LOCATION DATA AT ISSUE HERE.

The Court has repeatedly recognized that advances in technology must be considered in delineating the Fourth Amendment's protections, because the Court "'must assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *United States* v. *Jones*, 565 U.S. 400, 406 (2012) (quoting *Kyllo* v. *United States*, 533 U.S. 27, 34 (2001)). See also *id.* at 420 (Alito, J., concurring in the judgment) (same); *id.* at 415-418 (Sotomayor, J., concurring) (explaining why changes resulting from technology must be considered in applying the Fourth Amendment); cf. *Packingham* v. *North Carolina*, 137 S. Ct. 1730 (2017) (taking account, in applying the First Amendment, of Americans' use of new mediums of expression resulting from advances in technology).

In *Riley* v. *California*, 134 S. Ct. 2473 (2014), the Court held that the search-incident-to-arrest exception to the warrant requirement did not apply to the contents of cell phones, because digital technology enables the storage in these devices of vast quantities of personal information. "With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.' The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." *Id.* at 2494-95 (citation omitted).

This case again requires the Court to address the Fourth Amendment's protections in light of the changes resulting from Americans' pervasive use of digital technology.

A. Broad Categories Of Highly Sensitive Personal Information About Virtually Every American Are Now Routinely Possessed By Third Parties.

The pervasive use of digital technology in every facet of life has produced a dramatic change in how Americans store their personal information. Private papers kept in the home have been replaced by digital information stored with third-party service providers. And detailed personal information about individuals that previously could not be collected—because it simply was not possible to do so—is gathered and retained by the third-parties that provide the digital services on which Americans rely.

1. Individuals store a variety of different types of personal information with third-party providers:

- Emails and text messages have displaced physical letters as our principal means of written communication.[2] And both emails and text messages are stored "in the cloud" on computer servers under the control of the

[2] U.S. first class mail volume dropped by 50% between 2007 and 2016. U.S. Postal Service, *A decade of facts and fi*gures, https://about.usps.com/who-we-are/postal-facts/decade-of-facts-and-figures.htm. Email use has grown significantly. *E.g.*, The Radicati Group, Inc., *Email Statistics Report 2017-2021* (Feb. 2017) (projecting 269 billion emails per day worldwide in 2017), http://www.radicati.com/wp/wp-content/uploads/2017/01/Email-Statistics-Report-2017-2021-Executive-Summary.pdf;

service provider.[3] Written letters, by contrast, were stored at home or at another place under the control of the writer or recipient.

- Prior to the advent of digital technology, personal photographs and significant personal documents also were stored in the owner's home. Today, they are likely to be retained in digital, rather than physical, form—and even if they are stored locally in a laptop computer or other device, copies also are stored "in the cloud" on a service provider's server.[4]

---

[3] As the Court explained in *Riley*, 134 S. Ct. at 2491, "'[c]loud computing' is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself"; "users often may not know whether particular information is stored on the device or [on a server], and it generally makes little difference." For example, the contents of "gmail" email accounts are stored on servers controlled by Google; "hotmail" accounts on servers controlled by Microsoft; and "yahoo" accounts on servers controlled by that company. Storage of text messages varies by service provider: some providers do not retain copies of text messages. Others store messages for a limited period of time. U.S. Dep't of Justice, Retention Periods of Major Cellular Service Providers (Aug. 2010), https://www.aclu.org/files/pdfs/freespeech/retention_periods_of_major_cellular_service_providers.pdf.

[4] See note 3, *supra*; see also Pew Research Center, *Use of Cloud Computing Applications and Services* (Sept. 2008), http://www.pewinternet.org-/2008/09/12/use-of-cloud-computing-applications-and-services/; Deloitte, *Photo sharing: trillions and rising* (2016) ("2.5 trillion photos will be shared or stored online"), https://www2.deloitte.com/global/en/-pages/technology-media-and-telecommunications/articles/tmt-pred16-telecomm-photo-sharing-trillions-and-rising.html.

- The same is true of individuals' health and financial information. Records that formerly were kept in physical form at home are now likely to be digital, and stored remotely with service providers whether or not copies of the digital records are also stored locally. This information may be stored in the form of emails or email attachments; or as digital documents; or it may be stored with the company providing mobile application services ("apps") for which the information is relevant, such as a health or financial services. (And, as the Court observed in *Riley*, the more than one million apps extend far beyond health and finance to cover every conceivable need and interest—from politics, to addiction treatment, to romance and shopping. 134 S. Ct. at 2490. Each app collects and stores information relevant to the service it provides.).

Importantly, most service providers retain the right to access digital information stored in the cloud by their customers.[5] All of this highly personal information in the custody of third parties is therefore also accessible by those third parties.

2. Third-party digital service providers themselves collect and retain additional personal information relating to their customers in the course of providing services to those customers.

The cell site location information ("cell location information" or "CSLI") at issue in this case is one

---

[5] *E.g.*, *United States* v. *Warshak*, 631 F.3d 266, 286 (6th Cir. 2010).

example. As petitioner explains (Br. 3-4), cell phones access the telecommunications network by connecting to cell towers (also called "cell sites"). Each tower has several directional antennas that divide the covered area into sectors. The cellular service provider maintains a record of the tower and antenna with which a cellphone connects. Because the service provider typically knows the precise latitude and longitude of its cell towers, this data can be used to locate a user within the particular cell served by that tower and within a particular sector of that cell.[6]

CSLI's precision in pinpointing a cell phone's location depends on the size of the area served by the tower, the number of directional antennas on the tower (which determine the number of sectors), and the technology deployed on the cell tower.[7] In the last ten years, the number of cell sites has increased by 57%—a trend that is expected to continue.[8] And new technology is further improving the precision of cell location information.[9]

---

[6] Joseph Hall, *Cell Phone Tracking: Trends in Cell Site Precision* (Apr. 22, 2013), https://www.cdt.org/files/file/cell-location-precision.pdf; En Banc Brief of *Amicus Curiae* AT&T Mobility, LLC in Support of Neither Party, *United States* v. *Davis*, No. 12-12928 (11th Cir. 2014); Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, U.S. Attorneys' Bulletin 16, 19 (2011), http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf.

[7] See generally Hall, *supra* note 6.

[8] Cellular Telecomm. Indus. Ass'n, *Annual Wireless Industry Survey Results* (2017), https://www.ctia.org/docs/default-source/de-fault-document-library/annual-year-end-2016-top-line-survey-results-final.pdf?sfvrsn=2.

[9] Wireless providers have been augmenting their networks with many smaller cells, each with its own antenna. The areas

More, smaller cell sites with improved technology means more accurate location information—approaching or even exceeding the precision of the location information provided by the Global Position System tracking process before the Court in *Jones*. See 565 U.S. at 403 (50-100 feet, which equals 15-30 meters). Thus, "[w]hile it is still the case in rural areas that location derived from cell phone antennas is not comparable to GPS (10 meters), in a growing number of cases, especially in urban areas, location based on antenna location will approach GPS-level precision."[10]

---

served by these new cells are much smaller than those served by traditional cell towers, resulting in increased location precision. See Small Cell Forum, *Small Cells Market Status Report* at 4, Tables 2-2, 2-3 (2017), http://scf.io/en/whate_papers/ Market_status_report_June_2017_Special_edition.php (reporting that Industry analysts expect new small cell shipments in North America to exceed 290,000 in 2017, and to increase to over 550,000 by 2020); see generally Hall, *supra* note 6, at 5.

These small cells are called "microcells," "picocells" and "femtocells." The exact specifications for each term vary, but according to one source, microcells, picocells and femtocells provide service to areas of 200m-2km, 4m-200m, and 10m respectively. Dimitris Mavrakis, *Do we really need femtocells?*, SlashData Blog (Dec. 1, 2007), http://www.slashdata.co-/blog/2007/12/do-we-really-need-femto-cells.

[10] Hall, *supra* note 6, at 2. A 2011 report of the House Judiciary Committee summarized testimony before the committee explaining that "the precision of [cell location data] will vary widely for any given customer of the course of a day and, for a typical user over time, some of that data will likely have locational precision similar to that of GPS. Indeed, in urban areas where providers are using microcell technology, the level of precision for cell tower location data can include individual floors and rooms within buildings." H.R. Rep. 111-70, at 90 (2011); see also *ECPA Reform and the Revolution in Location-Based Technologies and Services: Hearing Before the Subcomm. on the*

Other service providers collect and retain detailed data regarding their customers' movements. Virtually every smartphone today contains a "map" feature that enables the user to find her location and obtain directions for reaching a specified destination. These features use cell site location data combined with data about WiFi access points to identify the user's location, and maintain a record of that location information.[11]

Service providers collect and retain many other types of personal information. For example:

Constitution, Civil Rights, and Civil Liberties of the House Comm. on the Judiciary, 111th Cong., 25 (2010) (testimony of Prof. Matt Blaze), http://judiciary.house.gov/_files /hearings/printers/-111th/111-109_5-7082.pdf.

[11] For example, the Google Maps Geolocation function returns location information based on data about nearby cell towers and WiFi access points. Google, *Google Maps Geolocation API*, https://-developers.google.com/maps/documentation/geolocation/intro. When a mobile device searches for a WiFi connection, it collects information about nearby WiFi access points. By recording the relative strength of WiFi signals, a device's location can be pinpointed based on the physical location of the WiFi access points stored in the database. *See, e.g.*, Skyhook, *Coverage Area*, http://www.skyhookwireless.com/-Coverage-Map; Kipp Jones, *Skyhook Under the Hood: Determining Location with Wi-Fi Access Points*, Skyhook (Mar. 11, 2015), http://blog.skyhookwireless.com/company/skyhook-under-the-hood-determining-location-with-wi-fi-access-points. See also Piotr Sapiezynski, et al., *Tracking Human Mobility Using WiFi Signals*, PLoS ONE 10(7) (2015), https://doi.org/10.1371/-journal.pone.0130824. These mapping features store the user's location information unless the user turns off the storage feature. Fred Zahradnik, *How to Find Your Location History in Google Maps or iPhone* (May 1, 2017), https://www.-lifewire.com/location-history-google-maps-iphone-1683392.

- Devices such as the Fitbit, which help users maintain physical fitness regimes, collect the user's heart rate, steps taken, and sleeping patterns.[12] Cell phones can be used to transmit medical information to doctors in real time.[13]
- Many individuals use services employing digital technology to control remotely home thermostats, smoke alarms, and other devices, as well as cameras to enable them to monitor their home's condition. These services record a variety of data, including when the home is occupied.[14]
- An individual's Internet browser retains a record of the websites that the individual visits—and much of that data is accessible by the individual's internet service provider.[15] Online advertisers deposit "cookies" in indi-

---

[12] Samuel Gibbs, *Jawbone's UP3 fitness device monitors heart rate to track sleep cycles*, The Guardian (Nov. 5, 2014); *Privacy Policy*, Fitbit, https://www.fitbit.com/legal/privacy (last accessed Jul. 25, 2017) ("When you use [the Fitbit], we collect data like number of steps you take or your [Body Mass Index] to show your stats and progress. And when you sync, we collect data like sync time and battery level, to help you keep your tracker (and yourself) up and running.").

[13] Eric J. Topol, *The Future of Medicine is in Your Smartphone*, Wall St. J. (Jan. 9, 2015), https://www.wsj.com/articles/the-future-of-medicine-is-in-your-smartphone-1420828632.

[14] Steven Melendez, *Nest is Learning to Detect When You're Home*, Fast Company (Mar. 10, 2016), https://www.fastcompany.com/3057706/nest-is-learning-to-detect-when-youre-home.

[15] *What ISPs Can See*, Upturn (Mar. 2016), https://www.teamupturn.com/reports/2016/what-isps-can-see.

viduals' Internet browsers that can be used to record the websites an individual visits.[16]

Prior to the invention and widespread use of digital technology, these detailed collections of highly personal information did not exist. Cf. *Jones*, 565 U.S. at 429, 430 (Alito, J., concurring in the judgment) (recognizing that "[i]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical"; and explaining that government officers "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").

In sum, digital technology has produced dramatic changes in the ways that Americans preserve their personal information and in the amount of personal information that is available. Those changes largely parallel the characteristics of cell phones described by the Court in *Riley*:

- The sheer amount of information is enormous—much more than any American could physically retain in the pre-digital era. Indeed, cloud computing allows the storage of limitless amounts of information, unlike a single cell phone which has a finite storage capacity.

---

[16] Chris Jay Hoofnagle, et al., *Behavioral Advertising: The Offer You Cannot Refuse*, 6 Harvard L. & Policy Review 273 (2012); Gunes Acar, et al., *The Web Never Forgets* (2014), Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (pp. 674-689), https://dl.acm.org-/citation.cfm?doid=2660267.2660347.

- The information is virtually always stored outside the home and in the custody of third parties—on servers "in the cloud."
- "[T]here is an element of pervasiveness that characterizes [digital data] but not physical records." *Riley*, 134 S. Ct. at 2490. As discussed above, the personal information held by third parties encompasses every aspect of an individual's life.

Just as the *Riley* Court took account of the changes wrought by digital technology in applying the search-incident-to-arrest doctrine, the Court in this case must take account of these realities in determining how the Fourth Amendment protects the privacy of highly sensitive personal information in the hands of third parties.

B. Fourth Amendment Principles Should Apply To Personal Information Held By Third Parties In A Manner That Recognizes The Realities Of Americans' Use Of New Technology.

A search within the meaning of the Fourth Amendment occurs when the government's conduct encroaches on an expectation of privacy "that society is prepared to recognize as 'reasonable.'" *Katz* v. *United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); see also *Jones*, 565 U.S. at 430 (Alito, J., concurring in the judgment); *id.* at 415 (Sotomayor, J., concurring); *Kyllo*, 533 U.S. at 33. That inquiry looks to the privacy expectations of "the hypothetical reasonable person"—"the average person's [privacy] expectations." *Jones*, 565 U.S. at 427, 429 (Alito, J., concurring); see also *Minnesota* v. *Olson*, 495 U.S.

91, 98 (1990) ("the every-day expectations of privacy that we all share").

The fact that an individual's personal information is held by a third party does not preempt this inquiry. This Court's precedents from the pre-digital era do not hold that a third party's possession of an individual's personal data by itself precludes a reasonable expectation of privacy with respect to that information. And the changes resulting from digital technology—with Americans storing vast quantities of personal information with third parties, and third parties creating databases of personal information not previously available—make it eminently reasonable to conclude that Americans have a legitimate expectation of privacy with respect to much of this information.

The circumstances surrounding the third party's acquisition and possession of the data may of course be relevant to the *Katz* inquiry. But the possession of information by a third party is not dispositive of the critical inquiry, which remains whether there is a reasonable expectation of privacy with respect to the information sought by the government.

1. Possession Of An Individual's Personal Information By A Third Party Does Not By Itself Exempt That Information From Fourth Amendment Protection.

The court below concluded that this case involves "business records obtained from a third party," and that the Court's decisions in *Smith* v. *Maryland*, 442 U.S. 735 (1979), and *United States* v. *Miller*, 425 U.S. 435 (1976), establish that petitioner could not have a reasonable expectation of privacy in the information contained in those records. Pet. App. 14a. That con-

clusion is wrong. Possession of an individual's personal information by a third party does not automatically preclude Fourth Amendment protection.

Neither *Smith* nor *Miller* rested exclusively on the third party's possession of the information—in both cases the Court also discussed the nature of the information at issue. The checks in *Miller* were "not confidential communications but negotiable instruments to be used in commercial transactions"; and both checks and deposit slips contain information "exposed to [banks'] employees in the ordinary course of business." 425 U.S. at 442. With respect to the dialed telephone numbers collected by the pen register at issue in *Smith*, the Court "doubt[ed] that people in general entertain any actual expectation of privacy in the numbers they dial," because they knew that the numbers were used to route calls, were recorded by the company, and were used by the company for a variety of purposes. 442 U.S. at 742.

To be sure, both opinions contain broad language referring to the lack of a legitimate expectation of privacy in information conveyed to third parties. *E.g.*, *Smith*, 442 U.S. at 743-44. But neither holding rested exclusively on that ground; each expressly addressed and relied on the particular nature of the information that was conveyed.

There is a vast difference between the narrow types of personal information addressed in *Smith* and *Miller* and the myriad categories and huge amounts of personal information that third parties hold today. See pages 7-15, *supra*. For that reason, "any extension of [those cases'] reasoning to digital data has to rest on its own bottom." *Riley*, 134 S. Ct. at 2489.

The Court should not extend *Smith* and *Miller* to this very different context. Holding generally that the Fourth Amendment does not protect an individual's personal information whenever that information is possessed by a third party would dramatically reduce the protection provided by the Fourth Amendment.

First, much of the information today held by third parties formerly was stored in an individual's home—such as private communications, pictures and documents containing personal information, and medical and financial information. To gain access to that information before the advent of digital technology, the government had to obtain a warrant. Holding that the Fourth Amendment does not apply if the information is in the hands of a third party would therefore eliminate the constitutional protection for this information, and very substantially reduce the protection for Americans' privacy.

Second, the detailed personal information generated in connection with services provided by third parties—an individual's location, everything she reads on the Internet, and her health data, to cite just a few examples—was not previously available to the government because it did not exist. There was no record of every newspaper, periodical and book that an individual read; or of every location an individual visited; or of a person's minute-by-minute physical condition. Permitting the government to obtain this information without a warrant would also therefore significantly diminish privacy protection. Accord, *Jones*, 565 U.S. at 428-30 (Alito, J., concur-

ring in the judgment); *id.* at 415-17 (Sotomayor, J., concurring).[17]

The *Riley* Court's observation with respect to the search of a cell phone's contents thus applies fully to a search by the government of personal data possessed by third parties: it would "typically expose to the government far more than the most exhaustive search of a house," because third parties "not only [possess] in digital form many sensitive records previously found in the home; [they] also [possess] a broad array of private information never found in a home in any form." 134 S. Ct. at 2491.

The government asserts that *Smith* and *Miller* stand for the broad principle that an individual can never have a reasonable expectation of privacy in information contained in a third party's "business records." Opp. 11-12. That is no limiting principle, however, because the term "business records" has no fixed meaning and therefore provides no guidance as to what types of information possessed by a business qualify as a "business record" and what types do not.

Indeed, the government argues in a related context that the contents of emails stored with an email service provider qualify as the provider's "business records." Pet. for a Writ of Cert. at 23-24, *United States* v. *Microsoft Corp.*, No. 17-2 (U.S. June 23,

---

[17] The government invokes (Opp. 24-25) the Stored Communications Act in arguing that Congress has provided appropriate privacy protection in this context. But that statute—enacted in 1986 and amended in 1994—preceded the sea change in Americans' use of third-party service providers. It therefore could not embody any determination with respect to the appropriate privacy protection in this dramatically different context. See pages 32-33, *infra*.

2017) (asserting that email contents constitute the service provider's business records and therefore must be produced pursuant to a subpoena served in the United States even if stored outside the United States). The government's rule therefore would sweep in all personal information in the possession of a third party—and therefore would result in the same very substantial reduction in Fourth Amendment protection.

2. Whether A Third Party Obtains Personal Information Through Individuals' "Voluntary" Acts Should Not Be Relevant To The Expectation Of Privacy Inquiry.

The Court's opinions in *Smith* and *Miller* observe that the information at issue in those cases was "voluntarily" provided to the telephone company and to the bank respectively. See 442 U.S. at 743-44; 425 U.S. at 442. Petitioner (Br. 39-44) and the government (Opp. 15-17) debate whether the location information at issue here was provided voluntarily or involuntarily.

Given the realities of today's digital environment, whether an individual provides information voluntarily should not be accorded any weight in the reasonable-expectation-of-privacy inquiry.

There simply is no correlation between the voluntary provision of information to a third party and legitimate expectations of privacy. Individuals voluntarily transfer the contents of emails, photographs, and sensitive personal documents to third-party service providers who store this information. Yet individuals believe, correctly, that absent unusual circumstances, this information will be private: it will not be viewed by anyone other than themselves or

persons who they authorize.[18] If voluntary provision of information alone precluded Fourth Amendment protection, this highly private information could be obtained by the government without a warrant.

Indeed, as the Court observed in *Riley*, individuals "often may not know" whether information is stored on their devices or on remote servers. 134 S. Ct. at 2491. And most experts advise individuals to store information remotely so that a problem with a cell phone, laptop, or other device will not mean that information will be permanently unavailable.[19]

Moreover, if voluntariness were somehow relevant, there can be no serious argument that the use of these services is any sense voluntary in today's world. Email services and a wide variety of other applications that encompass sensitive personal information are accessed via cell phones—and cell phones and the services they provide are now, as the Court recognized in *Riley*, "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude that they were an important feature of human anatomy." 134 S. Ct at 2484.

Data confirms the pervasiveness of Americans' use of these services: 95% own a cell phone of some type and 77% own smart phones; 80% of adults own laptop computers; and 50% of adults own tablet com-

---

[18] Although service providers retain the right to review emails, documents, and other materials stored with them, that right is limited and in reality virtually never takes place—and therefore does not diminish users' reasonable expectation of privacy. See, *e.g.*, *United States* v. *Warshak*, 631 F.3d at 286-88.

[19] Iron Mountain, Why Cloud Backup: Top 10 Reasons (2010), http://resources.idgenterprise.com/original/AST-0022659_top-_ten_reasons_cloud_backup.pdf

puters.[20] Nine-in-ten adults use the Internet; three-quarters have broadband service at home; and 80% shop on-line.[21] Americans spend an average of two and one half hours each day using Internet-based applications on their cell phones or accessing the Internet using their cell phones.[22] And "[t]he average smart phone user has installed 33 apps."[23] Utilizing these services is not voluntary—it is a necessity of modern life.

Finally, while "voluntarily" providing sensitive personal information to a third party should not preclude Fourth Amendment protection because of the changes in American's behavior and expectations resulting from digital technology, but involuntarily providing information should be a factor favoring such protection. If an individual does not know that she has imparted personal information, the fact that the information is in the possession of a third party should not be relevant to the Fourth Amendment inquiry—the individual's reasonable expectation of privacy would be the same as if the information had remained in her possession.

---

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

[21] Pew Research Center, Internet/Broadband Fact Sheet (January 2017), http://www.pewinternet.org/fact-sheet/internet-broadband/; Pew Research Center, *Online Shopping and E-Commerce*, http://www.pewinternet.org/2016/12/19/online-shopping-and-e-commerce/.

[22] Cellular Telecomm. Indus. Ass'n, *Wireless Snapshot 2017*, https://www.ctia.org/indusrty-data/ctia-annual-wireless-industry-survey.

[23] *Riley*, 134 S. Ct. at 2490.

3. The Legitimate Expectation Of Privacy Inquiry Should Turn On The Nature Of The Personal Information And Whether Individuals Would Reasonably Expect Their Information To Be Generally Available To Others.

The focus of the Fourth Amendment inquiry in the context of personal information in the possession of a third party should be no different than in other contexts: the question is whether the individual has a reasonable expectation of privacy with respect to that information.

Two basic factors are relevant.

The nature of the information sought. A court should assess whether the data sought encompasses sensitive personal information as to which there is a reasonable expectation of privacy. That inquiry would take account of the nature of the data, the volume sought, and what it would reveal about an individual—both alone and when combined with other information available to law enforcement officers.

The latter inquiry is particularly important. Digital technology enables the government to combine datasets with relative ease. Such cross-matching may reveal more personal information than each dataset standing alone. To take one elementary example, cross-matching information about an individual's movements with the businesses or individuals resident at the places that she stops could reveal extremely sensitive information. Repeated visits to an oncologist could reveal a health condition; visits to a political party office or other organization could reveal political or policy views.

But data matching can be much more sophisticated. Integrating even some of the numerous datasets in the hands of third parties could enable the government to learn many private details about a person's life. Cf. *Riley*, 134 S. Ct. at 2490 (the apps on an individual's smartphone "together can form a revealing montage of the user's life").

The circumstances under which the information was provided to the third party. A court should assess societal expectations regarding the general availability to others of the particular information provided to or obtained by the third party. That would include whether the information is subject to contractual, regulatory, statutory, or judicial limits on its dissemination by the third party. If the information was obtained involuntarily, that fact should weigh in favor of a reasonable expectation of privacy.

C. The Cell Phone Location Information Here Is Subject To The Warrant Requirement.

There is a reasonable expectation of privacy in 127 days of cell site location data showing the location of petitioner's cell phone during that period. Like the GPS tracking data at issue in *United States* v. *Jones*, this information was private prior to the advent of digital technology, because there was no way to collect it. Moreover, such detailed location data allows law enforcement officers to obtain extremely sensitive information about the most personal aspects of an individual's life. Finally, the circumstances under which the information was obtained, and the legal regime governing the third party's treatment of the information, confirm that there is a reasonable expectation in the information's privacy.

1. Location Data Reveals Highly Sensitive Personal Information.

The long-term cell phone location data obtained by the government is extremely sensitive information in which individuals have a reasonable expectation of privacy.

First, there is no doubt that data providing a cell phone's location for 127 days is the equivalent of information describing all of its owner's movements during that period. Indeed, the movements of a cell phone are more likely to parallel its owner's location than the movements of the car in *Jones*—individuals often park a car and walk to a different location, or series of locations, but it is rare indeed for an individual to be separated from her cell phone. *Riley*, 134 S. Ct. at 2490 (stating that "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"); see also *Commonwealth* v. *Augustine*, 4 N.E.3d 846, 861 (Mass. 2014) (observing that "because a cellular telephone is carried on the person of its user, it tracks the user's location far beyond the limitations of where a car can travel").

Second, the tracking of the phone, like the GPS tracking in *Jones*, provides a record of an individual's movements that law enforcement officers would not have been able to compile in the pre-digital era. To come close "would have required a large team of agents, multiple vehicles, and perhaps aerial assistance." *Jones*, 565 U.S. at 429 (Alito, J., concurring in the judgment) (footnote omitted).

And the task of tracking an individual would be much more difficult than tracking a vehicle—because

individuals are smaller and therefore harder to identify from afar; they more easily blend in with a crowd; and they can walk in and out of buildings, make sudden changes in their route, and take other actions that make tracking difficult. Therefore, it is even more true in this context that with respect to routine law enforcement investigations such as the robbery investigation here, "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 [phone] for a very long period." *Id*. at 430.

The court below found no reasonable expectation of privacy in the cell location data here in part because it determined that the cell location data was less precise than the GPS tracking data in *Jones*. Pet. App. 12a-14a. That conclusion is wrong for several reasons.

To begin with, even though cell location data may sometimes be less precise than GPS tracking, it is dramatically more precise than the information available to the government before the advent of digital technology—and that is the relevant comparison. Without digital technology, the government could not have compiled a 127-day record of petitioner's movements. And the fact that the government uses the data in court to place a defendant at the scene of criminal activity (See Pet. Br. 24-26) confirms that the information it provides is sufficiently precise to infringe on reasonable privacy expectations.

Moreover, the precision of cell location data varies based on the size of the cell, the number of antennas on the cell tower, and the particular technology used by the cell. In many urban areas, cell loca-

tion information today is just as precise as GPS information. As the number of cell towers increases, and new technology is deployed, GPS-level precision will be available broadly. See pages 9-11, *supra*.

In addition, long-term location data does not just infringe on the reasonable expectation that our daily movements will not be tracked by the government; it also enables the government to learn about the private aspects of a person's life. That is true of cell location information generally, which can be analyzed to determine particular locations and routes important to the individual.[24] Analysis of those locations and routes in turn can reveal religious affiliation, political affiliation, and other sensitive personal attributes.[25]

When cell location information approaches the accuracy of GPS tracking—as it increasingly does today—then it can reveal "a wealth of detail about [an individual's] familial, political, professional, religious, and sexual associations." *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).

Third, a constitutional test should not turn on the particular level of precision of the cell location data in this case. See *Kyllo*, 533 U.S. at 36 (observing that although "the technology used in the [case before the Court] was relatively crude, the rule we

---

[24] Sibren Isaacman et al., *Identifying Important Places in People's Lives from Cellular Network Data* (2011), http://mrm-group.cs.princeton.edu/papers/Isaacman_pervasive11.pdf.

[25] *E.g.*, Kai Biermann, *Betrayed by our own data*, Zeit Online (Mar 10, 2011) (personal information obtained when German Parliament member allowed newspaper to obtain his cell location data for one week), http://www.zeit.-de/digital/datenschutz/2011-03/data-protection-malte-spitz.

adopt must take account of more sophisticated systems that are already in use or in development").

Such a rule would be completely impractical. Officers could not know in advance where a particular individual had traveled or the particular level of precision of the cell site information in each of those areas. They accordingly would not know in advance whether the location information they would obtain with respect to their target would be at "GPS-level" or a lesser level of precision. The officers accordingly could not know in advance whether or not Fourth Amendment protection would be triggered.

Courts would be faced with difficult line-drawing issues. They would have to assess the level of precision in each of the cells at issue. Then they would have to determine whether the particular level of precision triggers the Fourth Amendment.

The *Riley* Court's rationale for rejecting a similarly vague test—permitting searches of cell phone contents where the information could have been obtained from a pre-digital source—is fully applicable to a level-of-geographic precision test for cell location information. Such a test "would launch courts on a difficult line-drawing expedition to determine which [cell location information is] comparable to [GPS information]. * * * It is not clear how officers could make these kinds of decisions before conducting a search, or how courts would apply the proposed test after the fact. [The] test would 'keep defendants and judges guessing for years to come.'" 134 S. Ct. at 2493 (citation omitted).

2. Individuals Would Not Reasonably Believe That Long-Term Location Data Would Generally Be Available To Third Parties.

The 127 days of location data relating to petitioner was held by third parties. It therefore is necessary to assess whether the circumstances under which the third parties acquired and retained the data undermine a reasonable expectation of privacy. They do not.

Creation of this data is an unavoidable consequence of using a cell phone. To the extent an individual wishes to have a cell phone—a necessity of life in today's world (see pages 21-22, *supra)*—location information will be collected and stored by the service provider. Whether or not a user knows that this takes place, and many, perhaps most, almost certainly do not,[26] the user has no choice.

Importantly, a cell service provider's dissemination of cell location information is strictly controlled. Federal law bars its disclosure without the customer's approval unless otherwise authorized by law. 47 U.S.C. § 222(c)(1), (f), (h)(1)(A). A number of States require law enforcement officers to obtain a warrant

---

[26] Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 Nw. U.L. Rev. 139, 177 (2016) (survey participants "were asked whether their cell phone service provider regularly collects information on their physical location using their cell phone. Nearly three-quarters of participants (73.5%) answered either 'No' (15.0%) or 'I Don't Know') (58.5%)"); see also *In re Application of U.S.*, 620 F.3d 304, 317 (3d Cir. 2010) (observing that "it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store" location information).

in order to access this information. Pet. Br. 22-23. These protections strongly support a reasonable expectation that the information would remain private.

The fact that the location information is possessed and accessed by a third party does not by itself vitiate the reasonable expectation of privacy. We already have explained why precluding Fourth Amendment protection for any information possessed by a third party would effect a very substantial reduction in Americans' privacy protection in light of the huge amount of personal information held by third parties due to the advent of digital technology. See pages 7-15, *supra*. The same result would follow from a rule withdrawing Fourth Amendment protection because the third party is authorized to access the information.

The Court has never endorsed the principle that an individual's decision to place information in a location in which it might be observed by another—or even to share private information with someone—vitiates a reasonable expectation of privacy in that information. Inviting guests into one's home does not relieve the government of its obligation to obtain a warrant, even if the information sought was in plain view of the guests.

Similarly, leaving private information in a hotel room—which is also accessible by the hotel owner—does not vitiate the expectation of privacy in that information. *Stoner* v. *California*, 376 U.S. 483 (1963). And the same is true of material placed in a safe deposit box, even though the bank has the ability and legal right to access the box on its own.

So too here. The ability of a cell service provider—or an email service provider, or the provider of

any of a myriad other digital services—to access the user's personal information under limited circumstances supports, rather than diminishes, the reasonable expectation of privacy with respect to that information.

This is not a situation in which an individual uses a digital medium to publish personal information to the world generally, or to a large group of individuals, or provides the information to a third party with knowledge that the third party will distribute it generally. To the contrary, the information here was generated as a consequence of using an essential service, and the use and distribution of the information is tightly restricted. Those facts enhance, rather than diminish, the reasonable expectation of privacy.

3. The Warrant Requirement Is Not Burdensome In This Context.

The Court has recognized 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. 2493 (citation omitted). Here, moreover, the warrant requirement will not impose any significant burden.

As the Court has noted, technological advances have "made the process of obtaining a warrant itself more efficient." *Ibid.*; see also *Missouri* v. *McNeeley*, 133 S. Ct. 1552, 1561-63 (2013).

Most importantly, the Stored Communications Act requires government officers to apply for judicial authorization to obtain cell location information without the customer's consent. 18 U.S.C. § 2703(c)(1). They may obtain either a warrant, or an

order based on a finding that "specific and articulable facts" show "reasonable grounds to believe that [the information sought is] relevant and material to an ongoing criminal investigation." *Id.* § 2703(d).

Because government officers already are obligated to obtain judicial process, requiring a warrant does not impose any additional procedural burden.

4. The Stored Communications Act Standard Does Not Satisfy The Fourth Amendment.

The government argues that the Stored Communications Act standard for government access to this information should control here—either because Congress made a determination to which the Court should defer, or because that standard satisfies the "reasonableness" requirement of the Fourth Amendment. Opp. 23-26. The government is wrong on both counts.

The congressional determinations embodied in the Act were made before digital devices became an essential part of Americans' everyday lives. The statute was enacted in 1986; and the government access provisions were last substantively amended in 1994. As petitioner explains (Pet. Br. 50), in 1986 few Americans owned cell phones and there were dramatically fewer cell towers—making cell location information both less of an issue for law enforcement and much less accurate. Congress could not have been focused on this issue when it enacted these statutory provisions.

Other provisions of the Act confirm this conclusion. To take just one example, the Act permits the government to obtain the contents of emails stored for longer than 180 days without obtaining a war-

rant; the government may use an administrative subpoena or a court order based on "reasonable grounds to believe" that the information is relevant to an investigation. 18 U.S.C. § 2703(a), (b), (d). Surely Congress did not—and could not reasonably—determine that Americans' privacy interest in emails, documents, and photographs automatically diminishes after 180 days. Rather Congress at the time did not, and could not, anticipate the revolution in the ways Americans retain personal information that has resulted from the pervasive use of digital technology.

The argument for an exception to the warrant requirement is similarly flawed. The Fourth Amendment's general requirement is that the law enforcement officers obtain a warrant, supported by probable cause, to conduct a search. "[E]xcept in certain carefully defined classes of cases, a search of private property without proper consent is 'unreasonable unless it has been authorized by a valid search warrant." *Camara* v. *Municipal Court*, 387 U.S. 523, 528-29 (1967); see also *McNeely*, 133 S. Ct. at 1558; *Kentucky* v. *King*, 563 U. S. 452, 459 (2011). An exception to this rule must be justified by special circumstances.

There are no such circumstances here. Federal law already requires recourse to a court, and exceptions to the warrant requirement generally turn upon the special burden on law enforcement that would result from requiring judicial intervention in particular circumstances. *McNeely*, 133 S. Ct. at 1559. Because officers already must obtain a court order, and the only question is the standard they must satisfy to obtain that order, there is no basis for creating a new exception to the warrant requirement here.

CONCLUSION

The judgment of the court of appeals should be reversed.

Respectfully submitted.

ANDREW J. PINCUS
Counsel of Record
Mayer Brown LLP
1999 K Street, NW
Washington, DC 20006
(202) 263-3000
apincus@mayerbrown.com

Counsel for Amicus Curiae

AUGUST 2017