NOTE: Where it is feasible, a syllabus (headnote) will be released, as is being done in connection with this case, at the time the opinion is issued. The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See United States v. Detroit Timber & Lumber Co., 200 U. S. 321, 337.

SUPREME COURT OF THE UNITED STATES

Syllabus

CARPENTER v. UNITED STATES

CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

No. 16-402. Argued November 29, 2017—Decided June 22, 2018

Cell phones perform their wide and growing variety of functions by continuously connecting to a set of radio antennas called "cell sites." Each time a phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI). Wireless carriers collect and store this information for their own business purposes. Here, after the FBI identified the cell phone numbers of several robbery suspects, prosecutors were granted court orders to obtain the suspects' cell phone records under the Stored Communications Act. Wireless carriers produced CSLI for petitioner Timothy Carpenter's phone, and the Government was able to obtain 12,898 location points cataloging Carpenter's movements over 127 days-an average of 101 data points per day. Carpenter moved to suppress the data, arguing that the Government's seizure of the records without obtaining a warrant supported by probable cause violated the Fourth Amendment. The District Court denied the motion, and prosecutors used the records at trial to show that Carpenter's phone was near four of the robbery locations at the time those robberies occurred. Carpenter was convicted. The Sixth Circuit affirmed, holding that Carpenter lacked a reasonable expectation of privacy in the location information collected by the FBI because he had shared that information with his wireless carriers.

Held:

DOCKE.

RM

1. The Government's acquisition of Carpenter's cell-site records was a Fourth Amendment search. Pp. 4–18.

(a) The Fourth Amendment protects not only property interests but certain expectations of privacy as well. *Katz* v. *United States*, 389 U. S. 347, 351. Thus, when an individual "seeks to preserve something as private," and his expectation of privacy is "one that society is

prepared to recognize as reasonable," official intrusion into that sphere generally qualifies as a search and requires a warrant supported by probable cause. *Smith* v. *Maryland*, 442 U. S. 735, 740 (internal quotation marks and alterations omitted). The analysis regarding which expectations of privacy are entitled to protection is informed by historical understandings "of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted." *Carroll* v. *United States*, 267 U. S. 132, 149. These Founding-era understandings continue to inform this Court when applying the Fourth Amendment to innovations in surveillance tools. See, *e.g.*, *Kyllo* v. *United States*, 533 U. S. 27. Pp. 4–7.

(b) The digital data at issue—personal location information maintained by a third party—does not fit neatly under existing precedents but lies at the intersection of two lines of cases. One set addresses a person's expectation of privacy in his physical location and movements. See, *e.g.*, *United States* v. *Jones*, 565 U. S. 400 (five Justices concluding that privacy concerns would be raised by GPS tracking). The other addresses a person's expectation of privacy in information voluntarily turned over to third parties. See *United States* v. *Miller*, 425 U. S. 435 (no expectation of privacy in financial records held by a bank), and *Smith*, 442 U. S. 735 (no expectation of privacy in records of dialed telephone numbers conveyed to telephone company). Pp. 7–10.

(c) Tracking a person's past movements through CSLI partakes of many of the qualities of GPS monitoring considered in *Jones*—it is detailed, encyclopedic, and effortlessly compiled. At the same time, however, the fact that the individual continuously reveals his location to his wireless carrier implicates the third-party principle of *Smith* and *Miller*. Given the unique nature of cell-site records, this Court declines to extend *Smith* and *Miller* to cover them. Pp. 10–18.

(1) A majority of the Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements. Allowing government access to cell-site records—which "hold for many Americans the 'privacies of life,'" *Riley* v. *California*, 573 U. S. _____ —contravenes that expectation. In fact, historical cell-site records present even greater privacy concerns than the GPS monitoring considered in *Jones*: They give the Government near perfect surveillance and allow it to travel back in time to retrace a person's whereabouts, subject only to the five-year retention policies of most wireless carriers. The Government contends that CSLI data is less precise than GPS information, but it thought the data accurate enough here to highlight it during closing argument in Carpenter's trial. At any rate, the rule the Court adopts "must take account of more sophisticated systems that are already in use or in

 $\mathbf{2}$

DOCKE.

development," Kyllo, 533 U.S., at 36, and the accuracy of CSLI is rapidly approaching GPS-level precision. Pp. 12–15.

(2) The Government contends that the third-party doctrine governs this case, because cell-site records, like the records in *Smith* and *Miller*, are "business records," created and maintained by wire-less carriers. But there is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers.

The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another. *Smith* and *Miller*, however, did not rely solely on the act of sharing. They also considered "the nature of the particular documents sought" and limitations on any "legitimate 'expectation of privacy' concerning their contents." *Miller*, 425 U. S., at 442. In mechanically applying the third-party doctrine to this case the Government fails to appreciate the lack of comparable limitations on the revealing nature of CSLI.

Nor does the second rationale for the third-party doctrine voluntary exposure—hold up when it comes to CSLI. Cell phone location information is not truly "shared" as the term is normally understood. First, cell phones and the services they provide are "such a pervasive and insistent part of daily life" that carrying one is indispensable to participation in modern society. *Riley*, 573 U. S., at ____. Second, a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the user's part beyond powering up. Pp. 15–17.

(d) This decision is narrow. It does not express a view on matters not before the Court; does not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras; does not address other business records that might incidentally reveal location information; and does not consider other collection techniques involving foreign affairs or national security. Pp. 17–18.

2. The Government did not obtain a warrant supported by probable cause before acquiring Carpenter's cell-site records. It acquired those records pursuant to a court order under the Stored Communications Act, which required the Government to show "reasonable grounds" for believing that the records were "relevant and material to an ongoing investigation." 18 U. S. C. §2703(d). That showing falls well short of the probable cause required for a warrant. Consequently, an order issued under §2703(d) is not a permissible mechanism for accessing historical cell-site records. Not all orders compelling the production of documents will require a showing of probable cause. A

DOCKE

warrant is required only in the rare case where the suspect has a legitimate privacy interest in records held by a third party. And even though the Government will generally need a warrant to access CSLI, case-specific exceptions—*e.g.*, exigent circumstances—may support a warrantless search. Pp. 18–22.

819 F. 3d 880, reversed and remanded.

ROBERTS, C. J., delivered the opinion of the Court, in which GINS-BURG, BREYER, SOTOMAYOR, and KAGAN, JJ., joined. KENNEDY, J., filed a dissenting opinion, in which THOMAS and ALITO, JJ., joined. THOMAS, J., filed a dissenting opinion. ALITO, J., filed a dissenting opinion, in which THOMAS, J., joined. GORSUCH, J., filed a dissenting opinion.

Opinion of the Court

NOTICE: This opinion is subject to formal revision before publication in the preliminary print of the United States Reports. Readers are requested to notify the Reporter of Decisions, Supreme Court of the United States, Washington, D. C. 20543, of any typographical or other formal errors, in order that corrections may be made before the preliminary print goes to press.

SUPREME COURT OF THE UNITED STATES

No. 16–402

TIMOTHY IVORY CARPENTER, PETITIONER v. UNITED STATES

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

[June 22, 2018]

CHIEF JUSTICE ROBERTS delivered the opinion of the Court.

This case presents the question whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements.

I

А

There are 396 million cell phone service accounts in the United States—for a Nation of 326 million people. Cell phones perform their wide and growing variety of functions by connecting to a set of radio antennas called "cell sites." Although cell sites are usually mounted on a tower, they can also be found on light posts, flagpoles, church steeples, or the sides of buildings. Cell sites typically have several directional antennas that divide the covered area into sectors.

Cell phones continuously scan their environment looking for the best signal, which generally comes from the closest cell site. Most modern devices, such as smartphones, tap into the wireless network several times

DOCKE

RM

DOCKET A L A R M



Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.