The United States Supreme Court Decides Privacy Issues Related to Cellular Phone Records

Law Enforcement Must Obtain a Search Warrant in Order Access Cell Phone Records from Cellular Providers

In *Carpenter v. United States*,[[1]](#footnote-1) the United States Supreme Court considered whether the Fourth Amendment was violated when investigators obtained a court order, rather than a warrant for cellular phone data that allowed investigators to place the defendant Carpenter in the vicinity of 4 robberies, after a co-conspirator confessed to the robberies and identified the involved subjects. At trial, the con-conspirators identified Carpenter as the leader of the pack.

The Court outlined the facts in *Carpenter* as follows:

In 2011, police officers arrested four men suspected of robbing a series of Radio Shack and (ironically enough) T-Mobile stores in Detroit. One of the men confessed that, over the previous four months, the group (along with a rotating cast of getaway drivers and lookouts) had robbed nine different stores in Michigan and Ohio. The suspect identified 15 accomplices who had participated in the heists and gave the FBI some of their cell phone numbers; the FBI then reviewed his call records to identify additional numbers that he had called around the time of the robberies.

Based on that information, the prosecutors applied for court orders under the Stored Communications Act to obtain cell phone records for petitioner Timothy Carpenter and several other suspects. That statute, as amended in 1994, permits the Government to compel the disclosure of certain telecommunications records when it “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.” [*18 U. S. C. §2703(d)*](https://advance.lexis.com/api/document?collection=statutes-legislation&id=urn:contentItem:4YF7-GPC1-NRF4-42Y4-00000-00&context=). Federal Magistrate Judges issued two orders directing Carpenter’s wireless carriers—MetroPCS and Sprint—to disclose “cell/site sector [information] for [Carpenter’s] telephone[ ] at call origination and at call termination for incoming and outgoing calls” during the four-month period when the string of robberies occurred. App. to Pet. for Cert. 60a, 72a. The first order sought 152 days of cell-site records from MetroPCS, which produced records spanning 127 days. The second order requested seven days of CSLI from Sprint, which produced two days of records covering the period when Carpenter’s phone was “roaming” in northeastern Ohio. Altogether the Government obtained 12,898 location points cataloging Carpenter’s movements—an average of101 data points per day.

Carpenter was charged with six counts of robbery and an additional six counts of carrying a firearm during a federal crime of violence. See *18 U. S. C. §§924(c)*, [*1951(a)*](https://advance.lexis.com/api/document?collection=statutes-legislation&id=urn:contentItem:4YF7-GN81-NRF4-4253-00000-00&context=). Prior to trial, Carpenter moved to suppress the cell-site data provided by the wireless carriers. He argued that the Government’s seizure of the records violated the *Fourth Amendment* because they had been obtained without a warrant supported by probable cause. The District Court denied the motion. App. to Pet. for Cert. 38a-39a.

At trial, seven of Carpenter’s confederates pegged him as the leader of the operation. In addition, FBI agent Christopher Hess offered expert testimony about the cell-site data. Hess explained that each time a cell phone taps into the wireless network, the carrier logs a time-stamped record of the cell site and particular sector that were used. With this information, Hess produced maps that placed Carpenter’s phone near four of the charged robberies. In the Government’s view, the location records clinched the case: They confirmed that Carpenter was “right where the . . . robbery was at the exact time of the robbery.” App. 131 (closing argument). Carpenter was convicted on all but one of the firearm counts andsentenced to more than 100 years in prison.

The Court cited some interesting background facts at the outset of their analysis to include that there are 396 million cell phone accounts in the United States though there are only 326 million people. The Court noted that cellular phones are constantly scanning the environment looking for the strongest signal, which generally comes from the closest cell site. Each time a cell phone connects to a cell site a time stamp record “known as cell-site location information” or CSLI is generated. The Court noted that these CSLI records are store by Cell Phone providers for five years.

The Court’s analysis in this case focused on the privacy of all citizens from government. In doing so, the Court reviewed how privacy and 4th Amendment interests have been viewed over time.

Fourth Amendment privacy was originally tied to the concept of trespass. Early cases focused on whether government actors, such as law enforcement had trespassed onto private property or constitutionally protected area to conduct a search. Thus the basic analysis was did law enforcement trespass upon private property? If they did so, did they have a warrant or in the alternative, did some exception the warrant requirement apply.

In 1967, the *Katz[[2]](#footnote-2)* case was decided. In *Katz*, there was no trespass to private property, but instead officers listened in to Katz’s conversations in a public phone booth. The Court found that listening to Katz private conversation in public phone booth violated the Fourth Amendment holding that the Fourth Amendment protects people and not places. Under this second type of Fourth Amendment privacy, which for lack of an identified term can be referred to as person privacy, the analysis is first; did the person exhibit a subjective expectation of privacy? If so, was that subjective expectation of privacy, one that society is willing to accept as a reasonable expectation of privacy.

It is clear from the facts of this case, that the Court would have to apply this second type of privacy analysis since there was no trespass onto private property in this case.

At the outset the Court noted that as technology has developed, it has become easier for government to pry into the private lives of citizens and thus the “Court has sought to ‘assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.” The Court noted that the Fourth Amendment “seeks to secure the ‘privacies of life’ against ‘arbitrary power… [and]… that a central aim of the Framers was ‘to place obstacles in the way of too permeating police surveillance.’”

The Court noted that cell phone records did not neatly fit into prior decisions and actually fit somewhat with two distinct lines of cases. One line of cases involves the level of privacy a person has in their physical location and movements and the second line of cases involves things a person keeps to themselves versus things a person shares with others. The second type has generally fund that information that a person voluntarily turns over to someone else has no legitimate expectation of privacy.

In its analysis the Court indicated that the application of the Fourth Amendment to the records obtained in this case was a “new phenomenon.” The Court rejected the application of the line of cases indicating that because these records are held by a third party, the cell phone provider, that there was no expectation of privacy.

Instead the Court focused on what private information could be gleaned from the constant and detailed location information received from these records. The Court noted that most people are never separated from their cell phone, even citing surveys of persons who indicate that they use their cell phone in the shower. The Court described that based on the records, government could determine a person’s religious affiliation by the location of the church they visited, their political affiliations by the locations they frequented, as well as their familial and sexual associations.

The Court cited the relative ease with which government could obtain information from cell phone providers and the fact that unlike other forms of surveillance that are conducted in real time, with cell phone data, law enforcement can go back in time to start their surveillance of an individual. The Court noted, with cell phone data, law enforcement does not even have to know in advance that they want to follow someone or when. “Whoever the suspect turns out to be, he has effectively been tailed every moment of everyday for five years, and the police may-in the Government’s view [which the Court rejects]—call upon the results of that surveillance without regard to the constraints of the Fourth Amendment. Only the few without cell phones could escape the tireless and absolute surveillance.”

The Court also asserted that in fashioning a rule in this case, the majority is recognizing that technology is advancing such that a person’s movements are becoming increasingly tracked and more accurate.

The Court concluded that when the government obtained Carpenter’s CSLI records from the telephone carriers, “it invaded Carpenter’s reasonable expectation of privacy in the whole of his physical movements.”

The Court rejected the government’s argument that the Fourth Amendment did not protect the cell phone records as third party business records and that Carpenter, in owning a cell phone, had voluntarily shared the information. The Court stated: “cell phones and the services they provide are ‘such a pervasive and insistent part of daily life’ that carrying one is indispensible to participation in modern society.”

The Court made clear:

“Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or “tower dumps” (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security. As Justice Frankfurter noted when considering new innovations in airplanes and radios, the Court must tread carefully in such cases, to ensure that we do not “embarrass the future.” [*Northwest Airlines, Inc. v. Minnesota, 322 U. S. 292, 300 (1944)*](https://advance.lexis.com/api/document?collection=cases&id=urn:contentItem:3S4X-3C00-003B-712V-00000-00&context=).

The Court held that law enforcement must generally get a warrant supported by probable cause in order to obtain the type of records obtained in this case. It was made clear that acquiring Carpenter’s records pursuant to a court order based on “reasonable belief” was insufficient to satisfy the probable cause requirement of a warrant.

Bottom Line:

When seeking cell phone records on an individual suspect, obtain a search warrant.

1. *Carpenter v. United States,*  \_\_\_S.Ct. \_\_\_; 2018 U.S. LEXOS 3844; (No. 16-402 Decided June 22, 2018). [↑](#footnote-ref-1)
2. *Katz v. United States,* 389 U.S. 347 (1967). [↑](#footnote-ref-2)