Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Carpenter And The High Court's Shift On 4th Amendment

By **Sarah Hall and Brian Lanciault** (July 23, 2018, 1:22 PM EDT)

Sarah Hall

Brian Lanciault

In a landmark decision issued on June 22, 2018, the U.S. Supreme Court held in a 5-4 decision that law enforcement must generally obtain a search warrant in order to obtain an individual's cell-site location information. The decision departs from the court's precedent, and curtails the ability of law enforcement to gather data and information about potential suspects from their wireless service providers. The decision continues a recent trend where the court has sought to take into account the ubiquity of technology in modern life and "ensure that the progress of science does not erode the Fourth Amendment" protections.

What Is Cell-Site Location Information?

Cell-site location information (CSLI) is geographic location information and call data (such as numbers dialed and call duration). CSLI is automatically captured by a cellular service provider when a cellular device is within range of a cellular service tower, or "cell site." Typically, a cellphone will scan the surrounding environment looking for the best signal and connect to the nearest source. When the cellphone connects to a cell site, a time-stamped location record is generated. More information may be gathered depending on whether the cellphone is used to make a call, send a text message or otherwise transmit data in the vicinity of the particular cell site. The accuracy of this information depends on the area covered by the cell site; a cluster of many cell sites in one area will typically have smaller coverage areas per cell site, resulting in more accurate location records.

The Facts of Carpenter v. United States

In 2011, the FBI arrested four men suspected of robbing a number of stores in Michigan and Ohio. One of the men confessed to his participation in the crimes and identified a number of accomplices, including Timothy Carpenter, and provided their cellphone numbers. Using that information, the government applied for a court order under the Stored Communications Act, 18 U.S.C. § 2703(d), to obtain the cellphone records of the accomplices. The Stored Communications Act authorizes a magistrate judge to issue a subpoena compelling production of cellphone records where the government shows "specific and articulable facts showing that there are reasonable grounds to believe" the records sought "are relevant and material to an ongoing criminal investigation."

The government subpoenaed records from Carpenter's wireless carriers, MetroPCS and Sprint, and obtained records spanning 127 days from MetroPCS and two days from Sprint. In the aggregate, the government acquired 12,898 location data points "cataloging Carpenter's movements" and placing him in the vicinity of at least four of the robberies. Carpenter was indicted in the Eastern District of Michigan. The government introduced Carpenter's CSLI as evidence at trial, and the prosecutor remarked in closing that it placed Carpenter "right where the ... robbery was at the exact time of the robbery."

Carpenter was convicted by the jury. He appealed, arguing that the government violated the Fourth Amendment when it obtained the CSLI, which, he claimed, constituted a search requiring a warrant. The Sixth Circuit affirmed the conviction and held that Carpenter lacked a reasonable expectation of privacy in the CSLI because he had shared that information with his wireless service providers.

The Core Question: Was There a Search?

The Supreme Court agreed with Carpenter, finding that the government's acquisition of the CSLI constituted a "search" within the meaning of the Fourth Amendment because it invaded Carpenter's "reasonable expectation of privacy in the whole of his physical movements." It went on to conclude that the government "must generally obtain a warrant supported by probable cause" to acquire CSLI records, and that the subpoena framework under the Stored Communications Act was insufficient because it did not require a showing of probable cause.

To reach its conclusion that the acquisition of the CSLI was a "search," the court sought to reconcile two parallel lines of doctrine: first, that an individual generally does not have an expectation of privacy in his physical location and movements in public, as held in United States v. Knotts (1983)[1] and recognized again in United States v. Jones (2012);[2] and second, that an individual has no expectation of privacy in information voluntarily conveyed to a third party, as established in Smith v. Maryland (1979)[3] and United States v. Miller (1976).[4]

Chief Justice John Roberts, writing for the majority, first looked to Knotts, which involved police tracking of a car using aerial surveillance and a "beeper" placed on an item that the defendant then unknowingly put into his car. The court observed that Knotts had expressly left open the question of whether dragnet-style "twenty-four hour surveillance of a[] citizen['s]" movements in public would be permissible under the Fourth Amendment absent a warrant. The court then turned to Jones, where police had placed a GPS tracker on a suspect's car and monitored the car's movements for 28 days. Although Jones principally held that the GPS tracking constituted a search because the government had "physically trespassed" on the defendant's property, the Carpenter majority observed that five justices had agreed that GPS tracking was "surveillance of the sort envisioned in Knotts," and that such "longer term GPS monitoring" would impinge on expectations of privacy — regardless of whether the person being monitored had disclosed such movements to the public at large.

The court concluded that individuals have a reasonable expectation of privacy in the whole of their physical movements as captured in CSLI. As support, the court noted the marked distinction between the cars in Jones and Knotts, and the cellphone at issue in Carpenter. A cellphone is "almost a feature of human anatomy" and "[w]hile individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time." The result — a "near perfect surveillance, as if [the government] had attached an ankle monitor to the phone's user."

The court then confronted the so-called "third-party doctrine." Under these rules, a person does not

have any expectation of privacy in information conveyed to a third party, and as a result, no "search" occurs when the government obtains that information. In Miller, the government subpoenaed the defendant's bank records, but the court declined to find a search had occurred because the defendant had neither "ownership nor possession" of the documents and freely conveyed them to the bank. In short, it concluded that the defendant had "take[n] the risk, in revealing his affairs to another," that the information revealed would "be conveyed by that person to the Government." Smith similarly concluded that the government's use of a "pen register" to record the telephone numbers dialed on a telephone implicated the same "risk" of disclosure because the user freely communicated the numbers dialed to the telephone company when using the phone.

The court expressly declined to extend Smith and Miller to a situation involving CSLI, which it deemed unique due to its "detailed, encyclopedic, and effortlessly compiled" nature. The court described the advance of technology as a "seismic shift" that created a "world of difference" from the sort of information at issue in Smith and Miller. This was not the sort of limited information typically at issue in third-party cases because CSLI was hardly "voluntarily" given — a premise of the third-party doctrine — due to the ubiquity and necessity of cellphone usage in modern times.

Thus, the court concluded that law enforcement's acquisition of CSLI constituted a search because an individual has a reasonable expectation of privacy in the whole of his or her physical movements as reflected in CSLI, and that expectation overcomes the application of the third-party doctrine in light of the unique character and content of CSLI.

Holding: The Government Must Obtain a Warrant

After concluding that a search occurred, the court went on to conclude that the government was required to obtain a warrant. Starting from the premise that a search is unreasonable under the Fourth Amendment absent a warrant, the court found the subpoena provisions of the Stored Communications Act were insufficient.

The court observed that a warrant will only be issued on probable cause, which requires some showing of individualized suspicion. But the Stored Communications Act fell "well short of" that requirement — requiring only that the information sought be relevant to an ongoing investigation, a much lower standard.

The court limited this holding, however, stating that a warrant was required "in the rare case" where a suspect had a legitimate privacy interest in records held by a third party. This seemed aimed at assuaging the concerns raised by the dissenters that the court had never before required a warrant when the government relied on subpoena processes to acquire records from third parties. Nor would a warrant be necessary in other familiar, exceptional and case-specific circumstances, such as those involving a fleeing suspect, an imminent risk of harm to the public, or the destruction of evidence.

Implications of Carpenter

Carpenter is a clear departure from other Fourth Amendment precedent involving information possessed by third parties and individuals' activities that occur in public. It questions the very premises on which those precedents were based in light of the type of information generated by modern technologies: broad, comprehensive and "encyclopedic" data concerning an individual's activities.

As cases continue to arise involving cellphones, GPS devices, and yet-to-be-invented technologies, the

court will continue to grapple with the proper application of the Fourth Amendment in our modern, technology-driven world.

Carpenter also is likely to generate more litigation involving the government's use of subpoenas. While the court attempted to cabin its holding as "a narrow one" and rebuke the dissent's concern that subpoenas would be rendered almost useless, the court's holding seems to actually invite this type of litigation. The standard articulated — that a warrant is required only "in the rare case where the suspect has a legitimate privacy interest in records held by a third party" — begs the question: will law enforcement know, in the midst of an investigation, whether a suspect has a legitimate privacy interest in the records it seeks? This would seem to open the door to after-the-fact litigation.

Individuals and businesses that may find themselves wearing the "third party" hat can prepare for this by understanding the types of information about individuals that they possess. Is it of the sort that might reveal the "privacies of life" or otherwise disclose the "whole of [a person's] physical movements"? As the court's opinion makes apparent, information that reveals personally identifiable information, physical location at regular time intervals, and other features of daily life, might very well qualify.

Conclusion

The court's decision in Carpenter carries on a more recent trend favoring privacy interests in our modern, technology-driven era. Rather than reflexively apply past precedent, the court is more solicitous of the nature and scope of the information involved. This approach in Carpenter led the court to depart from the traditional third-party doctrine, which had precluded an individual from claiming a reasonable expectation of privacy in information held by a third party.

Instead, the court has held that there is an expectation of privacy and a warrant is required for the government to obtain that information. The addition of the warrant requirement, where a subpoena had previously sufficed, will likely invite more disputes regarding third-party records subpoenas as litigants will quarrel over whether a suspect in fact had a legitimate privacy interest in the records sought. Defendants should therefore be prepared to raise and address these issues in the face of records subpoenas.

Sarah Hall is senior counsel and Brian Lanciault is an associate at Thompson Hine LLP.

[1] United States v. Knotts, 460 U.S. 276 (1983).

[2] United States v. Jones, 565 U.S. 400 (2012).

[3] Smith v. Maryland, 442 U.S. 735 (1979).

[4] United States v. Miller, 425 U.S. 435 (1976).