In a landmark decision, the United States Supreme Court holds the law enforcement officers need to obtain a warrant in order to gather a criminal suspect's cell phone location data

July 2018

Article Source : http://www.patc.com/weeklyarticles/2018_csli_chapman.pdf

In the first case that the United States Supreme Court has decided on the issue of law enforcement's use and gathering of cell-site location information (or "CSLI") on a criminal suspect's cell phone, the Supreme Court held that a warrant, supported by probable cause, is necessary in order to gather CSLI because the criminal suspect has a privacy interest in his physical location and movements.

At the beginning of its Opinion, the Supreme Court set forth the issue before it as follows: "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." The Supreme Court, then, noted the popularity of cell phones and gave a brief description of its technology. Specifically, the Supreme Court explained that each time a cell phone connects to a cell site, it generates a time-stamped record known as cell-site location information ("CSLI"). The precision of this information depends on the size of the geographic area covered by the cell site. The greater the concentration of cell sites, the smaller the coverage area. As data usage from cell phones has increased, wireless carriers have installed more cell sites to handle the traffic. That has led to increasingly compact coverage areas, especially in urban areas.

Wireless carriers collect and store CSLI for their own business purposes, including finding weak spots in their network and applying "roaming" charges when another carrier routes data through their cell sites. In addition, wireless carriers often sell aggregated location records to data brokers without individual identifying information of the sort at issue here. While carriers have long retained CSLI for the start and end of incoming calls, in recent years, phone companies have also collected location information from the transmission of text messages and routine data connections. Accordingly, modern cell phones generate increasingly vast amounts of increasingly precise CSLI.

Thereafter, the Supreme Court set forth the relevant facts for the appeal. In 2011, police officers arrested four men suspected of robbing a series of Radio Shack and T–Mobile stores in Detroit, Michigan. One of the men confessed that, over the previous four months, the group 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 the suspect's 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 Timothy Carpenter and several other suspects. That statute 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). 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. 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 of 101 data points per day.

Eventually, Carpenter was charged with six counts of robbery and with an additional six counts of carrying a firearm during a federal crime of violence. 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. 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 because they confirmed that Carpenter was right where the robbery was at the exact time of the robbery. The jury convicted Carpenter on all but one of the firearm counts and sentenced to more than 100 years in prison.

The Court of Appeals for the Sixth Circuit affirmed Carpenter's conviction and sentence. The Sixth Circuit held 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. Given that cell phone users voluntarily convey cell-site data to their carriers as "a means of establishing communication," the Sixth Circuit concluded that the resulting business records were not entitled to Fourth Amendment protection.

Upon this factual backdrop, the Supreme Court held that law enforcement's acquisition of Carpenter's cell-site records constituted a Fourth Amendment search. The Supreme Court opined that the Fourth Amendment protects not only property interests but certain expectations of privacy as well. 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 (1979). 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. The Supreme Court stated that these founding-era understandings continue to inform it when applying the Fourth Amendment to innovations in surveillance tools.

Furthermore, the Supreme Court stated that 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 of cases addresses a person's expectation of privacy in his physical location and movements. United States v. Jones, 565 U.S. 400 (2012)(five Justices concluding that privacy concerns would be raised by GPS tracking). The other set of cases addresses a person's expectation of privacy in information voluntarily turned over to third parties. United States v. Miller, 425 U.S. 435 (1976)(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).

The Supreme Court stated that 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, the Supreme Court declined to extend Smith and Miller to cover them.

Instead, the Supreme Court noted that a majority of the Court had previously recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements. Allowing the Government access to cell-site records—which hold for many Americans the privacies of life—–contravenes that expectation. In fact, historical cell-site records present even greater privacy concerns than the GPS monitoring considered in Jones in that 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 argued that CSLI data was less precise than GPS information, but the Supreme Court countered that the Government thought the data accurate enough to highlight it during the prosecutor's closing argument in Carpenter's trial. Regardless, the Supreme Court stated that the rule that it adopts must take account of more sophisticated systems that are already in use or in development while accounting for the fact that the accuracy of CSLI is rapidly approaching GPS-level precision.

Finally, the Supreme Court rejected the Government's argument 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 wireless carriers. The Supreme Court stated that 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. In mechanically applying the third-party doctrine to this case, the Supreme court found that the Government had failed 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 according to the Supreme Court. 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. 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.

Finally, the Supreme Court highlighted the fact that its decision was narrow. The Supreme Court refused to express a view on matters not before it, and it declined to disturb the application of Smith and Miller or to call into question conventional surveillance techniques and tools such as security cameras. Moreover, the Supreme Court did not address other business records that might incidentally reveal location information, and it did not consider other collection techniques involving foreign affairs or national security. Instead, the Supreme Court limited its opinion to CSLI and the need for obtaining a warrant in order to obtain that information.

In the end, the Supreme Court held that the Government did not obtain a warrant supported by probable cause before acquiring Carpenter's cell-site records. Instead, the Government 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." The Supreme Court determined that such a showing fell well short of the probable cause required for a warrant. Consequently, the Supreme Court held that an order issued under the Stored Communications Act is not a permissible mechanism for accessing historical cell-site records. Although not all orders compelling the

production of documents will require a showing of probable cause, the Supreme Court stated that a warrant is required in the 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, the Supreme Court concluded that case-specific exceptions—e.g., exigent circumstances—may support a warrantless search. Four Supreme Court Justices dissented from this Opinion.