FOURTH AMENDMENT

Carpenter v. U.S., --- U.S. --- (2018)
Decided June 22, 2018

FACTS: In the spring and summer of 2011, police apprehended four men accused of armed robberies in the Detroit area. One of the accused gave his own cellphone number to the FBI, as well as those of other participants. Call records were used to identify "still more numbers" of possible conspirators. The FBI applied for three orders to request "transactional records" for 16 numbers, from various wireless carriers. The accounts for Carpenter and Sanders were among those requested. The warrants were issued under the Stored Communications Act, 18 U.S.C. 2703(d), which allows such disclosure when the evidence provides reasonable grounds that the information would be "relevant and material to an ongoing criminal investigation." Using that information, gathered through an analysis of 127 days of back data, the conspirators were able to be localized to the area of each robbery, in varying levels of precision.

Carpenter and Sanders were charged with interstate robbery. They moved to suppress the cell-site evidence, claiming that probable cause was required for the disclosure. The District Court denied the motion. Both men were tried, and the cell site data for the two men was presented, with an agent testifying how the records indicated that both phones were in close proximity to the location of each robbery, at the time it occurred.

Both men were convicted, and appealed. The U.S. Sixth Circuit agreed that the federal courts have long made a distinction between the "content" of a personal communication and the "information necessary to get those communications from Point A to Point B." The initial cases, of course, applied to physical mail, but the law was eventually applied to telephone calls in the same way. Federal law now accords that same protection to email and similar communications, as well.[1] However, up to this point, the courts had not yet "extended those protections to the internet analogous to envelope markings, namely the metadata used to route internet communications, like sender and recipient addresses on an email, or IP addresses." The Sixth Circuit agreed that cell-site data, much like metadata in emails, was the "envelope" rather than the contents of a communication. As such, it was entitled to lesser privacy rights.

The Sixth Circuit agreed that such locational data was not subject to any expectation of privacy.[2] Any cell phone user understands that their location is being transmitted to a tower and that the carriers keep a record of the location from which calls are being made. These records are not extremely precise, as noted by the facts of the case – in which the phones could only be placed in a ½ mile to two mile radius.

---

[1] U.S. v. Warshak, 631 F.3d 266 (6th Cir. 2010).
[2] Smith v. Maryland, 442 U.S. 735 (1979).

The Sixth Circuit agreed that the business records of cell phone locations are not a search under the Fourth Amendment. Carpenter requested certiorari and the U.S. Supreme Court granted review.

ISSUE: Is a search warrant required for access to cell site location information for historical data?

HOLDING: Yes

DISCUSSION: The Court began with a review of the history of the Fourth Amendment, and its beginning being tied with physical intrusions on areas in which an individual expects privacy. In modern times, however, the concept of privacy has expanded beyond physical boundaries. When applying such principles to "innovations in surveillance modes," the Court faced a challenge to find a balance. Specifically, the court looked at Kyllo v. U.S.[3], which dealt with thermal imaging technology, and Riley v. California[4], which addressed the storage inside a cell phone. The Court acknowledged that it faced the hurdle of anticipating new technologies

The Court acknowledged that this case fell at the juncture of two Fourth Amendment doctrines: the issue of an expectation of privacy in information handed over to third parties In the first, in the past, a lesser expectation of privacy has been accorded traditionally, but "that does not mean that the Fourth Amendment falls out of the picture entirely." Although the information is provided voluntarily in one sense, the use of cell phones has become so pervasive that "carrying one is indispensable to participation in modern society." Unless the phone is disconnected from the network, there is "no way to avoid leaving behind a trail of location data."

The Court continued with a review of the technology of cell phone and how they might be located using cell phone tower triangulation. The tremendous power available to essentially track an individual's movements, precisely, as far back as one's cell phone carrier maintains records, was difficult to imagine even a few years ago. As in the issue with Kyllo, the less-precise technology today is likely to evolve into the more precise technology tomorrow. Although at the time the Carpenter case began, it acknowledged, the location of the cell phone could only be described in fairly general terms, that technology has continued to improve in the interim and can only be expected to continue to become more and more precise.

The Court also noted that cell phones have become "almost a 'feature of human anatomy'" with research indicating that the majority of individuals "compulsively carry cell phones with them all the time." Although vehicles may be left behind, the "cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." In fact, it equated to the government attaching an ankle monitor to the user. Further, using the cell-site location information (CSLI),

[3] 533 U.S. 27 (2001).
[4] 573 U.S. 2014.

the police could "travel back in time to retrace a person's whereabouts," limited only by the retention cycle of the carrier. Further, officers do not even need to decide who they wish to "follow" in advance. Certainly, cell-site records are business records, held by a third-party, but the cell phone companies are "ever alert, and their memory is nearly infallible," as the companies continually, and almost casually, collected an "exhaustive chronicle of location information."

The Court concluded that in this factual scenario, law enforcement must obtain a warrant, based upon probable cause – specifically to obtain historical location data on a cell phone user. However, the Court noted that the decision was to be construed narrowly and that "real-time CSLI" of a specific user or "tower dumps" – a "download of information on all the devices that connected to a particular cell site during a particular interval – triggered different possibilities. The Court also noted that it did not "consider other collection techniques involving foreign affairs or national security." It allowed that exigent circumstances would also apply and would justify not obtaining a warrant.

The Court reversed the Sixth Circuit Court of Appeals, and remanded the case for further proceedings.

Full Text of Decision: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf