Government's Acquisition of Cell-site Records is a Search Under the Fourth Amendment

Description

Today, the United States Supreme Court issued its decision in *Carpenter v. United States* (No. 16-402), 585 US ____ (2018), holding that when the Government obtains access to historical cell-phone records that provide a chronicle of the user's past movements, it constitutes a search under the Fourth Amendment. As such, the Government must generally obtain a warrant supported by probable cause before acquiring such records.

In 2011, police officers arrested four men suspected of robbing a series of Radio Shack and 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 obtained court orders issued by a magistrate judge under *Section 2703(d)* of the Stored Communications Act for cell phone records of the petitioner Timothy Carpenter and several other suspects. The Stored Communications Act (SCA) requires reasonable grounds to believe that the records sought are relevant to an ongoing investigation, which is lower than the probable cause standard under the Fourth Amendment.

In sum, the Government obtained 12,898 location points cataloging Carpenter's movements—an average of 101 data points per day. These records revealed that Carpenter used his cell phone within a half-mile to two miles of several robbery locations during the time robberies occurred. Carpenter was charged with six counts of robbery and an additional six counts of carrying a firearm during a federal crime of violence. Carpenter filed a motion to suppress the records, arguing that the government violated the Fourth Amendment by not obtaining a search warrant based on probable cause to obtain this information. The District Court denied the motion and Carpenter was convicted. Carpenter appealed the District Court's judgment to the Sixth Circuit Court of Appeals.

The Court of Appeals affirmed the District Court's decision. In doing so, it stated that the Supreme Court has long recognized a distinction between the content of a communication and the information necessary to convey it. Content is protected under the Fourth Amendment, but routing information is not. Consequently, the court held that the government's collection of cell-site records created and maintained by the defendants' wireless carriers was not a search under the Fourth Amendment. Carpenter appealed to the Supreme Court.

The Government argued that individuals, such as petitioner Carpenter, do not have a legitimate expectation of privacy in the business records that third-party service providers maintain of the location of cell towers used to route calls to and from cellphones.

Carpenter, on the other hand, argued that the government should be required to obtain probable cause warrants instead of 2703(d) orders issued under the Stored Communications Act to access historical

cell site location information from service providers because these records deserved heightened protection under the Fourth Amendment.

The issue before the Court is: 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.

A divided Supreme Court (5-4 ruling), rejected the Government's argument and reversed the Court of Appeals. The reasons are set forth below:

1. This case involves the Government's acquisition of wireless carrier cell-site records revealing the location of Carpenter's cell phone whenever it made or received calls. This sort of digital data—personal location information maintained by a third party—does not fit neatly under existing precedents. Instead, requests for cell-site records lie at the intersection of two lines of cases, both of which inform our understanding of the privacy interests at stake.
    1. a. The first set of cases addresses a person's expectation of privacy in his physical location and movements.
2. The Court had previously considered the Government's use of a "beeper" to aid in tracking a vehicle through traffic in *U.S. v. Knotts*, 460 U.S. 276 (1983), wherein police planted a beeper in a container before it was purchased by one of the defendant's co-conspirators. The officers were able to follow the signal from the beeper from Minneapolis to the defendant's cabin in Wisconsin. In the *Knotts* case, the Court concluded that the "'augmented' visual surveillance did not constitute a search because 'a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." The *Knotts* Court, however, was careful to distinguish between the rudimentary tracking facilitated by the beeping and more sweeping modes of surveillance. The Court specifically stated, "Different constitutional principles may be applicable if twenty-four hour surveillance of any citizen of this country were possible."
3. Three decades later, the Court addressed more sophisticated surveillance in *United States v. Jones*, 565 U.S. 400 (2012), which involved the installation of a GPS tracking device on Jones' vehicle, and remotely monitoring the vehicle's movements for 28 days. In the *Jones* case, the concurring Justices concluded that since "GPS monitoring of a vehicle tracks 'every movement' a person makes in that vehicle, . . . the longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy – regardless whether those movements were disclosed to the public at large."
    1. b. In a second set of decisions, the Court has drawn a line between what a person keeps to himself and what he shares with others. The Court stated that it has previously held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." That remains true "even if the information is revealed on the assumption that it will be used only for a limited purpose." As a result, the Government is typically free to obtain such information from the recipient without triggering Fourth Amendment protections.
4. This "third-party doctrine" stems from its decision in *U.S. v. Miller*, wherein the Government was investigating Miller for tax invasion and subpoenaed his banks, seeking several months of cancelled checks, deposit slips, and monthly statements. In *Miller*, the Court rejected a Fourth Amendment challenge to the records collections because 1) Miller could "assert neither ownership nor possession of the documents," as they were "business records of the bank;" and 2) the "nature of those records confirmed Miller's limited expectation of privacy, because the checks were 'not confidential communications but negotiable instruments to be used in commercial

transactions,' and the bank statements contained information 'exposed to [bank] employees in the ordinary course of business.'"

5. In *Smith v. Maryland*, 442 U.S. 735 (1979), the Court applied those same principles in the context of information conveyed to a telephone company. In *Smith*, the Court held that the Government's use of a "pen register – a device that recorded the outgoing phone numbers dialed on a landline telephone – was not a search." The Court noted that the pen register had "limited capabilities," and "doubted that people in general entertain any actual expectation of privacy in the numbers they dial." The Court further noted that subscribers were aware that telephone companies utilized this information for a variety of "legitimate business purposes," including routing calls. Further, when Smith placed a call, he "voluntarily conveyed" the dialed numbers to the telephone company by "exposing that information to its equipment in the ordinary course of business." In *Smith*, the Court found the defendant "assumed the risk that the company's records would be divulged to police."
6. In the present case, the Court stated that the question now confronted is how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals. Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled.
7. The Court noted the fact that the individual continuously reveals his location to his wireless carrier implicated the third-part principle set forth in *Smith* and *Miller*, but stated that "while the third-party doctrine applies to telephone numbers and bank records, it is not clear whether its logic extends to the qualitatively different category of cell-site records." "When *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements.
8. The Supreme Court declined to extend *Smith* and *Miller* to the present case, stating: "Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection. Whether the Government employs its own surveillance technology or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. The location information obtained from Carpenter's wireless carriers was the product of a search."
9. The Court further reasoned that an individual does not surrender all Fourth Amendment protection by venturing into the public sphere. A majority of the Supreme Court has previously held that "individuals have a reasonable expectation of privacy in the whole of their physical movements."
10. The Court found that although cell-site records are generated for commercial purposes, "that distinction does not negate Carpenter's anticipation of privacy in his physical location. Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the timestamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations. . . These location records hold for many Americans the 'privacies of life.'"
11. The Court distinguished the Government's tracking of an individual utilizing cell-records from the utilization of GPS records, as discussed in *Knotts* and *Jones*, by stating that "a cell phone – 'almost a feature of human anatomy' – tracks nearly exactly the movements of its owner. While individuals regularly leave their vehicles, they compulsively carry cell phones with them at all time. . . . Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user."

12. The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another. Cell phone location information, however, is not truly “shared” as one normally understands the term. In the first place, 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.
13. A cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily assume the risk of turning over a comprehensive dossier of his physical movements.
14. The Court held: “Given the unique nature of cell phone location information, the fact that the Government obtained the information from a third party does not overcome Carpenter’s claim to Fourth Amendment protection. The Government’s acquisition of the cell-site records was a search within the meaning of the Fourth Amendment.” Accordingly, “the Government must generally obtain a search warrant supported by probable cause before acquiring such records.”

Date Created
08/30/2018