Brief in Favor of the Respondent in Carpenter v. U.S. | Laura Jiang & Alex Li

In the Supreme Court of the United States

February Term, 2018

TIMOTHY IVORY CARPENTER, PETITIONER

V.

UNITED STATES OF AMERICA, RESPONDENT

ON WRIT OF CERTIORARI

TO THE UNITED STATES COURT OF APPEALS

FOR THE SIXTH CIRCUIT

RESPONDENT'S OPENING BRIEF

Laura Jiang & Alex Li

Counsel of Record

Lake Oswego High School

Room 213

Lake Oswego Oregon, 97034

(503) 534-2313

Counsel for Respondent

Oral argument: https://youtu.be/cw-k0kyACMc

QUESTION PRESENTED

DOES THE WARRANTLESS SEARCH AND SEIZURE OF CELL PHONE RECORDS INCLUDING LOCATION DATA OVER THE COURSE OF 127 DAYS

VIOLATE THE FOURTH AMENDMENT?

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

Other Authorities

Statement of Argument

The government's collection of cell phone data, including location data, is not a search of "persons, houses, papers, and effects" under the Fourth Amendment. As such, the Federal Bureau of Investigation's (FBI) data collection permitted under the discretion of a magistrate judge through the Stored Communications Act is constitutional. Katz v. United States also establishes the standard for "a reasonable expectation of privacy," where "first, a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" Precedent under U.S. v Miller establishes the third-party doctrine; records obtained from a third-party, in this case the retrieval of the petitioner's transactional records from his service provider, are not in violation of a reasonable expectation of privacy. While Katz v. United States clarified a "search" to include electronic intrusion, precedent set by Smith v. Maryland concludes that collection of transactional records and locational data is not considered a search under the Fourth Amendment, waiving the subsequent warrant requirement. The petitioner can claim no proper expectation of privacy as the cell phone user should know that dialed numbers and location data is kept by their respective carrier company. necessary for legitimate business purposes. By actively using his cell phone for communications while in the middle of several robberies, the petitioner did not demonstrate any reasonable expectation of privacy. It is clear that the government of the United States of America, the respondent, is not in violation of the Fourth Amendment.

Arguments

I. This collection of the Petitioner's cell phone data does not violate the Fourth Amendment's protection against "unreasonable search and seizures," as the petitioner does not demonstrate a reasonable expectation of privacy.

The first question to consider is whether the collection of transactional data, including location data of the petitioner, is considered to be a "search" under the Fourth Amendment. To answer this question, this Court must defer to the test established under Katz v. United States, determining whether the petitioner demonstrated a reasonable expectation of privacy and thus experienced a violation of their Fourth Amendment rights.

The Court has previously stated that "[l]egitimation of expectations of privacy by law must have a source outside the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." Within each application of the law, it is also important to note that the Court "must find resolution in the facts and circumstances of each case" to additionally consider the "reasonableness" standard. The activity in this case is that the FBI used the petitioner's phone number to collect 127 days worth of cell-data activity. Applying Smith, the nature of the activity was in regards to data collected from his cell phone provider and the petitioner cannot claim any violation or invasion of "property." In a similar case, the Court noted:

"Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed – a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers."

Although the petitioner's use of a cell phone and subsequent data collection is different from a pen register, the larger point made in Smith and United States v. New York Tel. Co. still stands. The "transactional records" obtained do not access any the content of any calls made by the petitioner, nor was the data actively collected by the FBI over a period of time —this was the collection of records at a single point of time of a mass of data that spanned 127 days. Any further claim of a "search or seizure" relies upon the an "expectation of privacy" regarding the numbers that the petitioner called and the location data gathered during the times in which he called other numbers from his cell phone—that is, while he was committing the robberies, not every single one of his phone calls or records.

The Court must reject this claim. First, there is no reasonable expectation of privacy in the numbers that an individual dials from their personal cell phone, nor would society generally recognise this information as private. The Court mentions:

"All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills."

The legitimate business interest in keeping these transactional records further proves there is no expectation from a subscriber to believe that these records of phone numbers dialed would be placed under a reasonable expectation of privacy.

II. **The Third-Party Doctrine allows the respondent to collect transactional data as established through precedent in Smith without diminishing any Fourth Amendment protections.**

The Court has established the third-party doctrine, stating:

"The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. . . . This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."

Given this, it is hard to place the petitioner's claims of expectations of privacy as reasonable. It is important to mention here that this application of the third-party doctrine does not represent a dramatic invasion of privacy nor does it drastically limit the protections of the Fourth Amendment. Justice Marshall mentions in Smith, "Privacy is not a discrete commodity, possessed absolutely or not at all." Those who adopt a doctrinalist view of the Fourth Amendment wrongly interpret privacy as an off-and-on switch, vastly oversimplifying the specificity of Carpenter's case; it is improper to assume privacy through "a conception of privacy as total secrecy."

To narrow the third-party doctrine would also significantly limit the abilities of law enforcement in future cases. Professor Orin Kerr of the USC Gould School of Law, who has written extensively on the third-party doctrine in his line of work, notes, "if at least part of a crime occurs in spaces unprotected by the Fourth Amendment, the police have at least some opportunity to look more closely at whether criminal activity is afoot." It is paramount that channels of communication remain open specifically in the context of data because of its usefulness in criminal investigations. He also notes the importance of the third-party as a method of balancing security and privacy:

"The third-party doctrine responds with a rule that ensures roughly the same degree of privacy protection regardless of whether a criminal commits crimes on his own or uses third parties. The part of the crime that previously was open to observation—the transaction itself—remains open to observation. The part of the crime that previously was hidden—what the suspect did without third parties in his home—remains hidden. The result leaves the Fourth Amendment rule neutral as to the means of committing the crime: Using a third party does not change the overall level of Fourth Amendment protection over the crime."

Second, while the petitioner may argue for a reasonable expectation of privacy when it comes to an individual's location of their cell phone, there is no expectation of privacy in regards to the cell phone towers that are built independent of cell phone users, nor would any rational subscriber conclude that the cell phone towers could be considered an individual's "property." In accordance with the third-party doctrine and dialed numbers, location data is similarly collected not for the purpose of tracking an individual's moment-by-moment location, but by necessity of connecting the individual to the cell phone tower for the purpose of calling, which was an activity taken by choice by the petitioner while the robberies were occuring.

While the petitioner discusses precedent which bans location tracking of an individual through the physical placement of a GPS, the circumstances of this case are different. In expert testimony from the Carpenter v. U.S. hearing in the United States Court of Appeals for the Sixth Circuit, it was stated that the radius for cell phone tower locations is 2.5 miles, a distance much more vague and non intrusive than the pinpoint accuracy achieved from a GPS satellite like the one installed in Jones. More importantly, while GPS signaling provides precise and constant tracking 24 hours a day, the FBI's collection of data is in regards to specific call records over the course of 127 days when the robberies had been occurring. The transactional records acquired specifically regarded incoming and outgoing calls, information obtained using the particular number that belonged to the petitioner. Therefore, there is a clear delineation between the tracking of Jones and the call records of this case. Consequently, claims of constant tracking made by the petitioner cannot be accepted. The Sixth District Court writes that the respondent collected "all subscriber information, toll records and call detail records including listed and unlisted numbers dialed or otherwise transmitted to and from [the] target telephones from December 1, 2010 to present[,]" as well as "cell site information for the target telephones at call origination and at call termination for incoming and outgoing calls[.]" Location data tracking only occurred when calls were placed, as opposed to the autonomous tracking that occurs through a GPS signal, distinguish Carpenter's case from Jones.

As such, the petitioner cannot claim to have an expectation of privacy in regards to the acquired location data, nor is there a societal expectation due to the conscious decision made by the petitioner to receive and make calls during the period of time in question.

III. The warrantless acquisition of the petitioner's transactional records was constitutional and legal, both through the procedural manner in which the data was acquired and because of the specificity of the data.

The third question is whether the collection of transactional records, without a warrant, is considered "unreasonable." Procedurally, under Katz, the opinion of the Court suggests the

FBi acted legally, utilizing the legal channels taken through the approvals of multiple magistrate judges. The Court writes:

"It is clear that this surveillance was so narrowly circumscribed that a duly authorized magistrate, properly notified of the need for such investigation, specifically informed of the basis on which it was to proceed, and clearly apprised of the precise intrusion it would entail, could constitutionally have authorized, with appropriate safeguards, the very limited search and seizure that the government asserts in fact took place."

The founding fathers' attempt to distance themselves from the oppression of the British Empire included the scrutinization and removal of oppressive writs. One such writ was the writ of assistance, implemented by the British government to expand the search power of its police. In his argument against unwarranted use of writs of assistance and greatly expanded police power, James Otis states:

"[I]n the old book, concerning the office of a justice of peace, precedents of general warrants to search suspected houses. But in more modern books you will find only special warrants to search such and such houses specially named, in which the complainant has before sworn he suspects his goods are concealed; and you will find in adjudged that special warrants only are legal."

Thus, the inclusion of specific warrants and legal channels are paramount to the safety and effectiveness of not only police, but the government as a whole. "Special warrants" are the check against tyranny in modern governmental systems, particularly the specificity of each warrant. Because of this, the specific legal channels cited in Katz—and that the FBI in this case followed—are important.

While the petitioner may believe there is an originalist interpretation of Fourth Amendment protections that would apply in this case, it is still not sufficient to rule in favor of Carpenter. In the unanimously adopted Virginia Declaration of Rights, George Mason, a prominent politician and delegate to the U.S. Constitutional Convention wrote,

"[G]eneral warrants, whereby any officer or messenger may be commanded to search suspected places without evidence of a fact committed, or to seize any person or persons not named, or whose offence is not particularly described and supported by evidence, are grievous and oppressive, and ought not to be granted."

The founding fathers understood their role in history and as such, knew that government ability to uphold the law was paramount, giving the government the constitutional authority to issue and utilize searches "particularly described and supported by evidence.

The Court's specific discussion of permissible procedure in Katz is consistent with the magistrate judges' approval of the FBI's examination of Carpenter's information under the Stored Communications Act. In the Court's delivered opinion for Katz, they mention:

"Only last Term we sustained the validity of such an authorization, holding that, under sufficiently "precise and discriminate circumstances," a federal court may empower government agents to employ a concealed electronic device "for the narrow and particularized purpose of ascertaining the truth of the . . . allegations" of a "detailed factual affidavit alleging the commission of a specific criminal offense."

In this instance, where the FBI's collection of transactional records was also necessary for "a specific criminal offense," the narrowly tailored surveillance committed by the FBI is legally and constitutionally justifiable. Under Katz, the Court was dealing with the question of wiretapping of conversations, and not the petitioner's transactional and location data obtained from a third-party. Such records hold at a lower standard of scrutiny in relation to privacy than individual surveillance of conversation. As such, the theoretically approved procedure according to the opinion of the Court and the lessened expectation of privacy in regards to the content of the data collected concludes that the FBI acted constitutionally and did not commit any violation of the petitioner's Fourth Amendment rights.

IV. The Court should defer to Congress and local legislation to determine the appropriate protections for cell-site data.

While the petitioner may claim that cell phones are "indispensable for full participation in family, social, professional, civic, and political life," a developmentalist view of the amendment is improper. It "risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." The Court has also offered that "technological equipment might have implications for future cases that cannot be predicted." In essence, ruling against the respondent would be too drastic a measure before we collectively can figure out the implications of technological innovation.

There is no need for the Court to create a bright-line test for cell-site data collection as there is no fundamental intrusion. Because the expectation of privacy is so minor in this case, this is an area best left explored by Congressional and other statutory law. In accordance with the relationship between business records and transactional data, it is preferable for legislative regulation under the Commerce Clause.

It is also imperative the Court not create too great a burden on law enforcement. The ease at which cell phones make criminal activity possible is immeasurable, thus raising the constitutional threshold for metadata searches ill advised. Technological changes have created many barriers to law enforcement ability, such as encryption leading to the iPhone dispute in 2016. The Department of Justice stated, "[i]t remains a priority for the government to ensure that law enforcement can obtain crucial digital information to protect national security and public safety, either within cooperation from relevant parties or through the court system with cooperation fails." Evolving cyber security necessitates a more potent and effective system of data collection that should not be significantly infringed on by the Court.

Conclusion

The collection of the petitioner's cell phone records does not violate the Fourth Amendment protections against "unreasonable search and seizure." Under the privacy test established by Katz v. United States, the petitioner fails to prove a "reasonable expectation of privacy" as the transactional records collected by the respondent are non-intrusive, nor are the unreasonable. The petitioner, by owning a cell phone, should recognise that they voluntarily surrender certain kinds of information to their cell phone service provider for business record collection purposes. These include call records and the location data that is necessarily recorded in order to connect the caller from their location to the nearest cell tower for the call to occur.

Under the third-party doctrine, the Court has previously held that information like transactional records are surrendered by the user of the service, in this case cell phones, and that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party." The cell towers, the ones in question that are responsible for transmitting location data within 2.5 miles, are not owned by the caller, meaning the petitioner cannot claim any sort of violation onto their "property."

In addition to these failed claims to privacy, the procedural manner in which the FBI acted was also perfectly constitutional and legal; the collection of the transactional data was carefully approved by multiple magistrate judges and an act of tailored surveillance. Dicta proves in favor of the respondent, where in Katz v. United States the Court mentioned that the actions of the government would have been constitutionally authorized had the government gone through the motion of magistrate judge approval. The narrowly tailored collection in this case follows a similar pattern of thinking, with the FBI actually having approval from magistrate judges.

Following the application of the privacy test and third-party doctrine, the intrusion is miniscule. Because of the Commerce Clause and legislation like the Stored Communications Act, the line for cell-data communication is best drawn by Congress. Overly broad rulings by the Court risk unknown consequences due to the limited knowledge regarding the potential for technology and its advancements. It is necessary that the Court recognise there is no fundamental basis for the Court to determine the limits of transactional record collection.

© 2021 The Harlan Institute. All rights reserved.