Harlan Virtual Supreme Court: Carpenter v. US- McDonnell and Lori

https://youtu.be/4maA7dK1emU

Petitioner's Brief – McDonnell and Lori

To be in the Supreme Court of the United States

November Term, 2017

TIMOTHY IVORY CARPENTER, PETITIONER

V.

UNITED STATES OF AMERICA, RESPONDENT

PETITIONER'S BRIEF

Christopher McDonnell & Zachary Lori

Counsel of Record

Greenwich High School

Room 528

Greenwich Connecticut, 06830

(203) 625-8000

Counsel for Petitioner

Oral argument: https://youtu.be/4maA7dK1emU

QUESTION PRESENTED

This case centers around the ability of the government to collect historical cell site location information (CSLI) without a warrant pursuant to the Stored Communications Act. 18 U.S.C §2703 (d) allows the government to get a court order to demand CSLI without demonstrating probable cause, but rather by offering "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication [...] are relevant and material to an ongoing criminal investigation." This lower standard for a court order has allowed the government to violate the fourth amendment protections of many americans, Timothy Carpenter included, for long periods of time. In this case the government used court orders pursuant to §2703 (d) to gather CSLI data for Carpenter for 127 days.

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

U.S. CONSTITUTION & STATUTES

OTHER AUTHORITIES

STATEMENT OF AUTHORITY

The Fourth Amendment of the Constitution is designed to protect ordinary citizens against abuse from the government in the form of unreasonable searches and seizures. New technology has reshaped the way law enforcement interacts with people and their property. The Court must recognize that many of the practical protections to privacy have been dissolved by modern technology. The application of the Fourth Amendment must change in order to continue to secure the privacy rights of everyday Americans. Incorporating an overly strict view of the third party doctrine that exempts all Fourth Amendment protections for information passed through a digital third party, as supported by the respondent, would be ill advised. It would weaken Americans' individual liberties and privacy rights well into the future, and ignore the legal roots of the doctrine. Furthermore, a complete invalidation of Fourth Amendment protections ignores how ordinary Americans interact with third parties on a daily basis. Our fundamental rights can only be protected if the third party doctrine is clarified to provide protection to sensitive information that might be gathered by a digital third party without being actively given to them. The warrantless subpoena of Cell Site Location Information is one form of a search that is unreasonable either through the lens of the third party doctrine, the broader Katz standard, or the original intentions of the Fourth Amendment.

ARGUMENT

1. HISTORICAL ARGUMENT

In the Virginia Declaration of Rights, George Mason wrote that "general warrants... are grievous and oppressive." In this vein, the Fourth Amendment of the United States Constitution bans general warrants. Today, CSLI data obtained by the federal government via the Stored Communications Act is worryingly similar to the general warrants disdained by the Founding Fathers. This is a concern voiced by legal minds such as George Washington University Law Professor Daniel Solove. A general warrant is defined as a warrant "providing a law-enforcement officer with broad discretion or authority to search and seize unspecified places or persons." When government officials request CSLI data over

a significant portion of time– for instance, 127 days– they can view the extremely broad range of places that a person tends to visit over a four-month timespan. When they request this data in 18 U.S. Code § 2703 (d) of the Stored Communications Act, as occurred in Carpenter's case, government officials do not need to meet the probable cause requirements for obtaining a warrant that are outlined in the Fourth Amendment. Instead, they can simply obtain a court order provided that the governmental entity offers "specific and articulable facts showing that there are reasonable grounds" to obtain the data given that it is relevant to an ongoing criminal investigation. The breadth of location information given to a government entity with a court order obtained via the Stored Communications Act is reminiscent of the "broad discretion… to search… unspecified places" of a general warrant.

The Fourth Amendment of the Constitution provides people the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures [...] and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." While the meaning of almost every word in this amendment has been reinterpreted over time, the fundamental principles and intentions of the Fourth Amendment remain mostly constant. The meaning of the wording changes as society progresses and there are new standards for what an "effect", or what is "reasonable". In the 1967 case Katz v. United States Justice Harlan's concurrence lays out the present standard for judging whether a search violates the Fourth Amendment. The first part of this standard is that the individual exhibits a subjective expectation of privacy. The second part of this standard is that society is prepared to recognize this expectation of privacy as reasonable. This standard is highly flexible, which means there are more specific standards for different types of potential Fourth Amendment violations.

The specific standard that applies to this case is the third party doctrine. The third party doctrine has evolved over time, and as said by Justice Blackmun in Smith v. Maryland (1979), "This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" (442 U.S. 773-774). However, although the respondent might wish to say otherwise, the third party doctrine has never been absolute. Nowhere in Smith did the Court say that information collected by a third party is given away inherently. Every case about the third party doctrine carefully examines what kind of information is being collected, and in what matter. There are even several cases where the rights of individuals to information collected by a third party are explicitly protected. For example in Ferguson v. City of Charleston (2001), the Court held that "[t]he reasonable expectation of privacy enjoyed by the typical patient undergoing

diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent" (532 U.S. 78). Although the majority did not directly mention the third party doctrine, it clearly contradicts a literal reading of the previous precedent, as recognized by Justice Scalia in his dissent where he said:

Until today, we have never held-or even suggested-that material which a person voluntarily entrusts to someone else cannot be given by that person to the police, and used for whatever evidence it may contain. Without so much as discussing the point, the Court today opens a hole in our Fourth Amendment jurisprudence, the size and shape of which is entirely indeterminate.

(Id. at 95). Justice Scalia is correct that Ferguson opens a hole in the third party doctrine, but this is not the first time that information arguably given voluntarily to third parties has been protected.

The Court has held that the content of phone calls is constitutionally protected, as in Katz v. United States (1967), even though they were willingly submitting their information through the infrastructure of a third party in order to relay their message to their intended recipient. United States v. Jacobsen (1984) held that "letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy" even though they are voluntarily entrusted a third party mail carrier. These cases do have distinct differences from the case of Carpenter, but they demonstrate that the third party doctrine is not as absolute as the respondent may wish to claim. Individuals can still retain a reasonable expectation of privacy over certain types of information and objects they voluntarily entrust into the care of a third party.

II. GENERATING CSLI DATA IS NOT VOLUNTARY

If the Court wishes to view this case from the perspective that it falls under the current Smith-based third party doctrine, the Court should still rule in favor of protecting CSLI data. The degree to which someone is voluntarily giving over information to a third party is central to the third party doctrine. In the beginning of the third party doctrine, with cases like Hoffa v. United States (1966), Hoffa willings chose to say incriminating statements to someone who happened to be a government informant. This informant then gave that information to the police. In cases like this, it is clear that the information was freely given. "[H]e was relying upon his misplaced confidence that [the informant] would not reveal his wrongdoing" (385 U.S. 302). Hoffa was not only fully aware that the traditional third party was listening to him, he was only revealing this information so that he could share it with them. This is an example of truly voluntarily conveyed information that should lack any expectation of privacy.

Over time the meaning of 'voluntary' has expanded well beyond what Hoffa and cases like it implied. United States v. Miller (1976) expanded the definition of voluntary, and limited the expectation of privacy, by saying that information he was forced to give to achieve his primary goal of sending a check, was also given voluntarily. Smith v. Maryland (1979) expanded the reach of the third party doctrine even further to allow it to rule over cases where information was not even knowingly given to a human. This transition from a traditional third party to a digital one is certainly marked and should not be understated. However, both of these cases are easily distinguishable from Carpenter's case.

In Miller, they were handing over information that they knew would be "exposed to [the bank's] employees in the ordinary course of business." (425 U.S. 443). There is no such human contact when CSLI data is transmitted. Furthermore, as Miller recognized, "checks are not confidential communications, but negotiable instruments to be used in commercial transactions" (Id. at 442) Miller wanted the bank to use the information he actively provided them in order to do something besides just relay the information. In Carpenter's case, he expected the phone line to provide him with an easy way to make calls. The only information he actively provided to make this service possible was the numbers he wished to call. When he received calls he lacked even this much input, because the CSLI data was created before he even picked up his phone.

Smith can also be distinguished with similar reasoning. Smith had to actively chose to enter in the numbers he wished to call, and he had to be aware that his phone company needed these numbers in order to accomplish his intended goal of completing the call. However, in Carpenter's case, as mentioned previously, he never actively provided his location, and he likely did not even know that his cell phone company was collecting his location information, as will be discussed shortly.

Expanding this doctrine even further to include CSLI data, which is both more sensitive and less voluntarily given than the previous cases, would be a mistake. Smith had to manually enter the number he wished to call into his phone, and Miller still had to physically hand over a check with all the routing information clearly visible to a banker in order to make his transaction. Not only is CSLI data not explicitly given when someone places a call, but, as other lower courts have recognized, "historical CSLI is also generate by passive activities such as automatic pinging, continuously running applications ("apps"), and the recept of calls and text messages." (2015 N.D. Cal. Opinion, 119 F. Supp. 3d 1024).

Furthermore, not only is this information not actively given, but a vast majority of people are not even aware of its existence. As the amicus curiae brief by the Empirical Fourth Amendment Scholars states, "In one recent study, only 26.5% of American cell phone users expressed even a general awareness that their cell phone companies may track their

locations. [...] Even with the most liberal coding—any response that could reasonably be interpreted as referring to cell site location tracking was counted as doing so—only 12.7% of this "Yes"-answering subset could be deemed to have been referring to cell-site tracking" This means only 3.4% of respondents showed a general awareness that cell phone companies track their locations through CSLI.

This empirical evidence is critical to assessments of knowledge because judges are more knowledgeable about the functions of government and how law enforcement functions. By the time they decide a case about fourth amendment protections they are also substantially more informed about the subject matter than an ordinary citizen. Without referencing empirical evidence, and the tendency of people to project their knowledge onto others, several lower courts have come to the conclusion that "users know that they convey information about their location to their service providers when they make a call and that they voluntarily continue to make such calls" (In Re U.S. For Historical Cell Site Data 724 F.3d 612 (2013)). This is evidently not the case given the empirical evidence, but even if societal knowledge about CSLI data changes, as all societal knowledge is prone to do, the usage of a cell phone in modern society will still not be truly voluntary.

Today, owning a cell phone is necessary for a member of modern American society. As Justice Roberts noted in the Court's opinion in Riley v. California (2014), "modern cell phones... are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." (573 U.S. ____) In 2015, 92% of Americans owned a cell phone, a higher percentage than that of Americans who own cars (88%). Privately-owned cars are indispensable to the modern American worker– 86% of workers get to work with one every day. Cell phones' are of similar importance to today's labor force. 53% of 18 to 29 year olds, who have the fewest established workplace connections, have used a smartphone to look for employment. Many employers also use text message and mobile apps to coordinate employee schedules. Services such as When I Work and ZoomShift require rapid communication to call an employee in or out over text message, while apps such as Shyft are used to exchange shifts between co-workers. The gig economy, which has been described as "Pioneering the Future" by Forbes Magazine, has also increased the necessity of cell phones. 60% of gig economy workers say that income earned through gig economy apps is either "important" or "essential" for meeting basic needs.

Cell phones are also essential for safety purposes. 70% of 911 calls are made via cell phone, which is underscored by the fact that 52% of American households do not have traditional landline phones but instead use cellular devices for telephonic communication. Cell phones have been proven to save lives. Authors of a recent study in the Journal of Emergency

Medicine found that "the use of mobile phones to alert emergency services in a life-threatening situation is associated with improved
mortality rates at the scene in patients with medical problems and a lower likelihood of admission to the emergency department." The overwhelming majority of Americans view cell phones as invaluable means of protection. 91% of American adults and 93% of teens agree that they "feel safer because [they] can always use [their] cell phone to get help." Cell phones are most essential for the poorest Americans, who are compelled to use them to access the Internet in lieu of expensive computers. Among American households who earn less than $20,000 a year, 63% of people who used their smartphone to access to internet said it is their primary way to access the internet.

III. CSLI DATA IS HIGHLY SENSITIVE

Cell Site Location Information should also be protected because of how sensitive it is. As the Court recognized in Riley v. California (2014), "nearly three-quarters of smartphone users report being within five feet of their phones most of the time" (573 U.S. ___). This fact must also be considered in combination with the fact that "even if the network only records cell tower data, the precision of that data will vary widely for any given customer over the course of a given day, from relatively less precise to relatively very precise, and nether the user nor the carrier will be able to predict whether the next data location collected will be relatively more or less precise. For a typical user, over time, some of that data will likely have locational precision similar to that of GPS." Modern phones also broadcast their location extremely frequently. They passively send out a 'registration signal' to nearby cell towers once every seven seconds, which can generate CSLI data. 82 % of Americans think that the details of their physical location over time is either very or somewhat sensitive information. It is evident that CSLI data is highly sensitive and must be protected.

The government itself has also recognized how people have a reasonable expectation of privacy about their CSLI data in 47 U.S.C.§ 222(c)(1), (f), (h)(1)(A), which mandates that telecommunications carriers must keep customer information private unless the government mandates they turn it over or the customer consents to releasing it. "[W]ithout the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to – cell location information." (47 U.S.C.§ 222(f)). Separately, 47 U.S.C. § 1002 (a)(2)B) says that although telecommunications carriers must be able to store and provide call identifying information pursuant to a court order, "with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices [...] such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the

extent that the location may be determined from the telephone number).” The testimony of Louis J. Freeh, the Director of the FBI at the time, reveals the intent behind this section. He said:

[Some people are] alleging that the government is seeking a new, pervasive, automated “tracking” capability. Such allegations are completely wrong. [...] In order to make clear that the acquisition of such information is not being sought through the use of a pen register or trap and trace device, and is not included within the term “call setup information”, we are prepared to add the concluding phrase to this definition to explicitly clarify the point: [above quote from § 1002 (a)(2)B)].

Both of these federal codes show that the government recognizes that customers have a reasonable expectation that their call identifying information will be private, especially their location data revealed from this call identifying information.

IV. THIRD PARTY DOCTRINE REFORM

The third party doctrine fundamentally functions as a shortcut to establish whether someone has a reasonable expectation of privacy. We would contend as Justice Sotomayor did in United States v. Jones (2011) that, “it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.” (565 U.S. 417). In the seven years that have passed since this was written the dangers of the third party doctrine have become even more apparent. Technology has removed all practical limits on how much personal information people can store, and it has also created new types of information that are highly sensitive. This Court shared this sentiment in Riley v. California (2014) where Chief Justice Roberts wrote, “The United States asserts that a search of all data stored on a cell phone is “materially indistinguishable” from searches of these sorts of physical items. [...] That is like saying a ride on horseback is materially indistinguishable from a flight to the moon” (573 U.S. ___). However, this information is increasingly stored on servers owned by private companies, called “cloud servers.” Certain types of computers, called “chromebooks” operate with minimal hard drive space, often around only 16 GB, and store the majority of their documents and files in Google Drive, a cloud storage system. The new Google Pixel 2 provides unlimited photo storage through another one of Google’s cloud storage systems: Google Photos. Ordinary people may not be able to distinguish between what files are physically stored on their phones, and what is stored on a digital third party’s servers, especially with the recent trend of “cloud backup” storage, which are services that store your information in a separate server, so that if your personal hardware malfunctions and corrupts your data, you can retrieve it.

This Court should not rule that these vast amounts of personal information, from photos to emails to health data, is unprotected simply because it is exposed to a digital third party. A much more nuanced third party doctrine should be established that determines a reasonable expectation of privacy based on the intended recipient of the information. If information is directly given to someone, with the sole intent that they receive it, like in Hoffa v. United States (1966) where information was intentionally given to the informant, then the third party doctrine will be unaffected by this new perspective.

However, if information is given to a digital third party for the sole intention that the store that information, like a cloud storage provider, or that they relay that information to a select group of individuals, like an email provider, then the person would have a reasonable expectation of privacy. The current view of the third party doctrine does not distinguish between something posted on a public twitter account and on a private twitter account, even though the information shared on each of those will be vastly different because the person sending it believes their message will be kept much more private in the latter.

Undoubtedly, this will decrease the capability of law enforcement to catch potential criminals. CSLI data is very frequently used by police to establish probable cause. In 2014 AT&T received 64,703 requests for CSLI data. However, protecting our fundamental right to privacy is more important than a small increase in the rate of catching criminals. In the words of Benjamin Franklin, "Those who would give up essential liberty to purchase a little temporary safety, deserve neither liberty nor safety."

CONCLUSION

The world is rapidly changing, and the Supreme Court must recognize that our fundamental Fourth Amendment protections are being seriously infringed upon because of the unconstitutional federal statute 18 U.S.C §2703 (d), which allows the government to relatively easily intrude into the private lives of Americans in a way that the founding fathers would despise. A vast majority (82%) of Americans think their location information is sensitive, but only 3.4% of them are aware that cell phone companies can track them through their CSLI data. The expansion and rapid integration of cellular technology into modern life means that even if they were aware that CSLI data was being collected, they still would not be making a voluntary choice to use a cell phone.

This points to a more fundamental problem with the third party doctrine. This court should recognize how ordinary people interact with digital third parties and make clear that they do not sign away all their fundamental right to privacy when they chose to send an

email through Google's servers, or backup their files with a cloud storage system, or own a cell phone that transmits their location every seven seconds. People interact with digital third parties on a daily basis with rationally different levels of privacy. This court should realize that some information passed through a digital third party can be expected to be private, while other information can be expected to be public. This court should not need to overturn traditional third party doctrine, such as that of Hoffa v. United States (1966), which has not been impacted by the rapid changes in modern technology.
