Sarah Mason and Delaney Ericson Petitioner Brief

Petitioner Brief – Mason and Ericson

In the Supreme Court of the United States

October Term of 2018

Timothy Ivory Carpenter

United States of America

Petitioner's Opening Brief

Sarah Mason and Delaney Ericson

Counsel of Record

Lake Oswego High School

Lake Oswego, Oregon

Counsel of Petitioner

Oral argument: https://youtu.be/aUTaqL5sWPc

Table of Contents (page numbers might be off because this was done in google docs)

Table of Cited Authorities

Cases

Other Sources

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?

Statement of Argument

The search of Timothy Carpenter's cell phone records constitutes a search that requires a warrant based upon probable cause. United States v. Jones 565 U.S. 400 (2012), clearly articulates that long term tracking of people is unconstitutional. The third party argument says that searches can be done without a warrant, if the information gathered could also be seen by another party. However, this does not stand, as precedent shows the high level of information stored on cellular devices does not allow for the third party exception. The magistrate judges in this case allowed the FBI to use information on the cell phones, such as historical cell site location information, after a confession brought forward other members of the crime's cell phone numbers. The magistrate judges allowed this under the Stored Communications Act , 18 U.S.C.§ 2703(d), which states that "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." The lack of "specific and articulable facts" comes from the matter that information was gathered over the course of 127 days rather than a singular, specific moment. This brings forward the fear of general search warrants

that were made under writs of assistance during colonial times, prompting the creation of the fourth amendment.

1. Historical Evidence

Although James Madison was not a proponent of adding a Bill of Rights, a push from the anti-federalists led to its creation. Of the rights listed, the fourth amendment granted a person's protections from government interference. The fourth amendment written by James Madison, in "Bills of Rights as Proposed" (March 4, 1789) declares, "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures". It arose from the fear that colonists had against writs of assistance which served as general search warrants. James Otis, declared "As this writ of assistance is. it appears to me . . . the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of the constitution, that ever was found in the English law-book" in Arguments Against Writs of Assistance (February 1761). In a case decided in an English court, Entick v. Carrington Lord Camden wrote " The great end for which men entered in society was to secure their property, that right is preserved sacred and incommunicable in all instances where it has not been taken away or abridged by some public law for the good of the whole...By the laws of England, every invasion of privacy, be it ever so minute, is a trespass" in the case of Boyd v. United States 116 U.S. 616, the Supreme Court declared Entick a guide to understanding the Fourth Amendment. Our Fourth Amendment is founded on the importance of retaining one's privacy even if that may impede the accessibility of law enforcement to information that helps them in criminal cases. Intrusions to privacy were a common complaint of the colonists, as written in a letter to the farmers and planters of Maryland in 1788, "Nay, they often search the clothes, petticoats and pockets of ladies or gentlemen (particularly when they are coming from on board an East India ship), and if they find any the least article that you cannot prove the duty to be paid on, seize it and carry it away with them; who are the very scum and refuse of mankind, who value not their oaths, and will break them for a shilling." The right to be secure in your effects without fear of unreasonable search and seizure was established early on in America's history, and clearly is still a relevant fear, as police execute warrantless searches of private phone records and data, in a way most similar to the unfounded searches of the people mentioned in the letter. In the Virginia Declaration of Rights George Mason declared, "[General 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." This indicated the fears of warrants lacking a specific scope and purpose. In the case before us, while the police did have evidence and probably would have probable cause to receive a warrant, the search was

not directed at a particular "place to be searched." Rather, it was conducted over a long period of time at various locations. The Massachusetts Declaration of Rights stated, "Every subject has a right to be secure from all unreasonable searches, and seizures of his person, his houses, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation; and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the persons or objects of search, arrest, or seizure: and no warrant ought to be issued but in cases, and with the formalities, prescribed by the laws." In the case of Carpenter, the police did not have a warrant, although they had the probable cause to obtain one, which is a clear violation of the spirit of the Massachusetts Declaration of Rights. With the police searching cell phone records without a warrant, Carpenter's protection from unreasonable searches was breached, as was the admissibility of the evidence obtained in this illegitimate search. In the New York Ratification Convention Debates and Proceedings (July 19, 1788), "[E]very freeman has a right to be secure from all unreasonable searches and seizures of his person, his papers, or his property; and therefore that all warrants to search suspected places, or seize any freeman, his papers or property, without information upon oath, or affirmation of sufficient cause, are grievous and oppressive; and that all general warrants (or such in which the place or person suspected, are not particularly designated) are dangerous and ought not to be granted." The question brought up here in Carpenter v. United States is whether this search was reasonable. Does the reasonable person believe that the police have the authority to track the location, association, and the actions of people without a warrant for a long period of time? This sounds like the "dangerous" general searches mentioned above. The private information of the inner workings of one's day, gathered through the historical cell site location information, should not be able to gathered without a warrant.

II. Expectation of privacy in precedent is in favor of the Petitioner

In Katz v. United States 389 U.S. 347 (1967), the court established the standard commonly referred to as, "expectation of privacy." In the case of Katz, the unwarranted wiretap of a phone was ruled as unconstitutional, based on the premise that telephone conversations are assumed to be private. In Carpenter, law enforcement did not intrude into conversations, but the details of one's location throughout the entire day are just as sensitive as one does not expect an infiltration into this area. Contrast this with the case of California v. Greenwood 486 U.S. 35 (1988), where garbage cans on the curb are not considered private because the public can see the contents. The garbage can, does not move, however, unlike Carpenter, who was in the public eye, but did not stay stationary. The moment that one steps out into the public eye, they give up enormous amounts of privacy. The house

remains one of the most guarded areas from governmental interference. In the case of Kyllo v. United States 553 U.S. 27 (2001), law enforcement used a thermal imaging device to detect the growth of marijuana, but was also able to track movement of the people inside the home, which was a gross violation of the fourth amendment. The search of Carpenter's phone records was unconstitutional as it gave police long-term information about Carpenter's location that the public would not know. In the case before us, the government is altering their view as well, while the cell phone site location information were within a public area, the public does not follow a person throughout their day. The question here is what level of privacy did the petitioner, Timothy Carpenter have. The contents of the cell phone record were not searched, but the ability to track a person throughout their daily movements is a horrific violation into one's privacy. People have the ability to see Carpenter at these locations, so how much privacy should he be awarded to where he is, the answer remains the level of privacy is still high enough where a warrant needs to be issued, as even close relationships do not know where a person throughout their entire day. There is a great concern about the "watching eye" of the government's ability to track a person's movement with little safeguards to stop them, if this case is ruled in favor of the United States. In California v. Ciraolo 476 U.S. 207 (1986), the court held that a private plane flown over one's backyard was not a violation because as quoted by Chief Justice Berger, "took place within public navigable airspace" as commercial airplanes would be able to see what law enforcement could. Carpenter differs as law enforcement is not able to see a person's movements unless they were tracking them by foot. Law enforcement is altering their view by being able to advance their vision with modern technology. The ruling in Ciraolo was affirmed in the case of Florida v. Riley 488 U.S. 445 (1989), in which a helicopter was used to the same effect where the public eye was able to see the same way as law enforcement. In the case of United States v. Davis 754 F. 3d 1205 (11th Cir. 2015), the eleventh circuit held that obtaining the information was done through the good faith exception established in United States v. Leon 468 U.S. 897 (1984). Using the good faith exception, may be prevalent in this case, but cannot stand for each case where historical cell site location information is gathered. In Davis, the court ruled that one's cell phone location was within one's reasonable expectation of privacy. Lastly, in Oliver v. United States 466 U.S. 170 (1984), the open field doctrine applied because people have no legitimate expectation of privacy in the open, but this is not an open field, if they can track every movement without a warrant, it becomes an open planet.

III. The need for a warrant is necessary.

In the case of United States v. Watson 423 U.S. 411 (1976), Justice Powell delivered a concurring opinion where he says that always requiring a search warrant can unnecessarily impede local enforcement. Clearly pointing to the fact that exceptions to the warrant

requirement are a necessary component of our judicial system, but there is a limit to how far exceptions go before they "eat the rule". This is one instance where an exception gives too broad of an authority. In Terry v. Ohio 392 U.S. 1 (1968), an exception allowed a short-term pat down of people without an arrest or warrant. The police in New York's "stop and frisk" policies went too far and targeted minority groups. The same could be said of this where it leads to law enforcement tracking one's movement with little safeguards. In Ex parte Jackson, 96 U.S. 727 (1878) the court ruled that the government needed to have a warrant to search the contents of the letters. They could view what was on the outside of the envelope because it was within the eye of the postman. This relates to our case as a warrant should be required before the police can search something that is out of their eyesight, as Carpenter's cell phone data was. In Stanford v. Texas, 379 US 476 (1965) the court ruled that the protections of the fourth amendment are guaranteed in the states as well by the fourteenth amendment. Although this was elaborated as well in Mapp v. Ohio, 367 US 643 (1961), it also mentioned that states may not constitutionally issue general warrants as well as anything that infringes upon the first amendment shall not be issued. While the first amendment statement is not prevalent in this case the general warrant part is. In this instance the tracking of Carpenter was extremely broad. The search was one that did not state a specific time or place to be searched. In Berger v. New York 388 U.S. 41 (1967), explained that a New York statute (N.Y. Code of Crim. Proc. § 813-a) violated the fourth amendment because the electronic eavesdropping in this case was allowed without any safeguards. This parallels with our case as a warrant was not issued to safeguard against law enforcement interaction. Magistrate judges used the Stored Communications Act to allow the collection of the information, but once again this is not the same as a warrant issued upon probable cause, but offers significantly less protection. In Carpenter the Stored Communications Act 18 U.S.C.§ 2703(d) did not follow the "specific" facts to watch a person's movement through cellular information over the course of 127 days. Also, the Stored Communications Act , 18 U.S.C.§ 2703(d) was not adequate to qualify for the search that occurred. It is unconditional to have a search of this magnitude without a warrant and done by magistrate judges. To gather historical cell site location information, a warrant granted by a court judge upon probable cause needs to be issued. In a case decided by a Massachusetts court, Commonwealth v. Estabrook 472 Mass. 852 (2015), ruled that historical cell site location information was accessible if it was within the time frame of six hours claiming that longer term is not permissible. Later on in Commonwealth v. Augustine 472 Mass. 448 (2015) in which they declared that a warrant upon probable cause must be issued if this information is to be gathered which takes away even the six hour possibility. In a New Jersey court, State v. Earls 70 A. 3d 630 (N.J. 2013), the court held that the gathering of cell site location information should require a search warrant unless it fits under one of the existing exceptions, such as a search incident to lawful arrest, consent of the search, or during an emergency/hot pursuit. It is important to note that in these

state court decisions there is an added layer of complexity which is state constitutions. State constitutions retain the ability to extend one's rights meaning that cell site location information collection may be a violation under state authority rather than the fourth amendment. In United States v. United States District Court of for the Eastern District of Michigan 407 U.S. 297 (1972), the court held that government officials must obtain a search warrant prior to beginning electronic surveillance even if domestic security issues are involved such as in our case with the bank robberies, as the search did not fall under any of the exceptions to warrantless searches. Safety versus freedom is a value tenison constantly present in our society. But if the founding fathers felt the need to secure our papers and effects through the fourth amendment (even though it might give up some safety) that truth should remain today. It cases such as these safety is not an justifiable excuse to go forward with a search lacking a warrant.

IV. Third Party Doctrine is not applicable.

The court has established third party doctrines, which state that if there are documents or data held by a third party, the people do not have expectation of privacy to those materials. However, in other cases involving technology the boundaries of the third party rule are not always perfectly clear. In US v. Miller 425 US 435(1976), the court reversed the fifth circuit's ruling that the collected bank records of Mitch Miller were not a violation of the fourth amendment because the bank was a third party, and therefore Miller had little expectation of privacy. Justice Powell explained, "documents subpoenaed are not [Miller's] 'private papers'. This is precedent establishing the third party rule which allows for such a search without a warrant. The difference is that in Carpenter the court relies on the decision of Riley v. California 573_(2014) which established that in an search incident to arrest the police would need a separate warrant to search the phone based on the vast information that phone contains. The court has decided that the information contained on cell phones has massive amounts of data; therefore, raising the expectation of privacy and making it an object with an expectation of privacy that needs a warrant. In another third-party case, Smith v. Maryland 442 US 735 (1979), the court ruled that cell phone pen registers are not protected as clients voluntarily provide the numbers to telephone companies meaning that it is not an infringement to gather this information without a warrant. However, Carpenter did not voluntarily give his cell phone company the location of his every move for a long period of time. In this case, the government clearly infringed on a an area that does have a reasonable expectation of privacy. Riley v. California 573 U.S._(2014) determined that warrants are necessary for data on smartphones, as they hold so much personal information. That data, stored with cloud computing is not even on the phone itself. As cloud computing is clearly a third party, it follows that a warrant is required to obtain records of a person's data. In Carpenter, his locations were obtained in a

warrantless search a third party's data, but in this case the third party was not cloud computing but cell towers, which have just as much personal information as a person's cloud data, as cell towers hold copies of text messages, calls, and keep track of the phone's location and should be granted just as much protection as such. While City of Ontario v. Quon 560 US 746 (2010) does conclude text messages can be searched, the difference between this case and Carpenter was that the phone in question being searched was a city-issued phone, and the city explicitly stated that it reserved the right to "monitor and log all network activity including email and Internet use, with or without notice". Carpenter's phone was privately owned, and therefore the decision reached in City of Ontario v. Quon 560 US 746 (2010) has no holding. In United States v. Warshak 631 F.3d 266; 2010 WL 5071766; 2010 U.S. App. LEXIS 25415, it was determined that it is in violation of the Fourth Amendment to compel someone's Internet service provider to turn over emails without a warrant. Much like in Carpenter, third parties with data relating to both phones and computers hold a huge amount of sensitive personal information, and people should feel secure that authorities should have to follow the same guidelines in searching his or her Internet service provider, cell phone company, or any other third party containing personal data as the authorities follow in searching his or her own person. Finally, in United States v. United States District Court for the Eastern District of Michigan 407 U.S. 297 (1972), the court held that before government can begin "electronic surveillance" a warrant needs to be obtained even if domestic security issues such as border or cyber security are present. We would urge the court to follow this precedent as the records gathered without a warrant are clearly electronic surveillance of a person.

V. Technological Safeguards in favor of Carpenter

Carroll v. US 267 US 132 (1925), established what became known as the automobile exception, the court ruled that automobiles can be searched without a warrant if there is probable cause of evidence in the car. This was coupled with the exigent circumstance that a vehicle could be removed before a warrant was issued. The mobility of the car established the need for this exception. The difference in this case is that records remain. A phone company cannot drive away records, meaning that the police have ample time to obtain a warrant. On a related note, in Riley v. California 573 U.S._(2014), the phone was not allowed to be searched, in part because police had the ability to keep the cell phone in a faraday bag which protects against remote erasure until a warrant is made. In a unanimous decision, United States v. Jones 565 US 400 (2012), Justice Antonin Scalia wrote the decision of the court which establishes that the installation of a global positioning system device on Jones' car was a violation of the fourth amendment based on the trespass of personal property. The court rejected the government's argument that people do not have any expectation of privacy in a person's movement in public areas. Justice Sotomayor also

wrote a concurring opinion in Riley which stated that she agreed that the government invaded Jones' privacy, but also important for when a government intrudes in an area of privacy that people reasonable expect. She points to the fact that in an era where many forms of surveillance are not physically intrusive. Sotomayor also mentioned during oral argument ""What motivated the Fourth Amendment historically was the disapproval, the outrage, that our Founding Fathers experienced with general warrants that permitted police indiscriminately to investigate just on the basis of suspicion, not probable cause, and to invade every possession that the individual had in search of a crime." She then asked, "How is this different?" (Sotomayor). Today we ask the same question: how is Carpenter different from the fears of the founding fathers. Bennett Stein, a legal assistant of the American Civil Liberties Union is quoted, "While Jones involved attachment of a GPS device to a car, its reasoning applies with even greater force to cell phone tracking. People carry their cell phones with them all the time. Each time a cell phone makes or receives a call or text message, the wireless provider logs the cell towers the phone connected to during that communication" (Stein). The poignant words from a defender of civil liberties shows the connection of Jones and Carpenter even though it is not exactly the same legal question. While the court did determine that planting a radio tracking device did not violate Fourth Amendment rights in United States v. Knotts 460 US 276 (1983), this does not relate to Carpenter. A radio tracker does not have nearly the same amount of information as a cell phone's GPS location, and Chief Justice Roberts himself said that using a beeper still took "a lot of work" whereas a GPS device allows the police to "sit back in the station ... and push a button whenever they want to find out where the car is." The two are not on the same level technologically speaking, and therefore should have different standards for warrantless searches. While United States v. Karo 468 US 705 (1984) established that a tracking device inserted into a container didn't constitute as a seizure, the difference between a tracking device and cell phone data is the tracking device only goes to one location, and does not have anywhere near the same amount of information as personal cell phone data, meaning this ruling has no effect on Carpenter. Arizona v. Gant 556 US 332 (2009) established a search of a vehicle after an arrest was only permissible if the suspect had access to the vehicle at the time of the search or if there was evidence pertinent to the arrest. Clearly, once he was arrested, Carpenter would have no ability to change his cell phone location data, and therefore a warrantless search of such was not only unnecessary, it was a clear violation of his Fourth Amendment rights.

Proposed Standard

The fourth amendment clearly outlines the need of a warrant that is required in cases such as this one. Without one, it is evident that the search was unreasonable. We propose that to

gather historical cell site location information, the police need to obtain a warrant which shall be issued upon probable cause.

Conclusion

Timothy Carpenter's fourth amendment rights were violated. A search of cell phone records that consisted of a period of 127 days was conducted without a warrant. The police had the capability of getting a warrant without fear that their evidence would slip away. The government intruded into an area in which a reasonable person would have an expectation of privacy. Allowing a search such as this will lead to a slippery slope, such as tracking someone's location through their cell phone GPS regardless if they have been suspected of a crime, where governments can easily monitor its people with few, if any, troubles.
