Old Dominion University

Carpenter v. United States:

Approaches of Privacy

Alysia Beckles

CYSE 406: Cyber Law

Professor Jude Klena

15 Oct. 2021

Alysia Beckles

Professor Jude Klena

CYSE 406

15 Oct. 2021

**Approaches of Privacy**

People do not only consider the reason for an investigation happening but how an investigation is being conducted. There have been many questions on how to carry out investigations when it concerns people’s privacy. Maintaining one right to privacy is imperative, but when regarding investigations, how do investigators or courts prevent themselves from infringing on people’s privacy rights. Although these concerns have yet to be alleviated with the introduction of everchanging, technology the problem persistently arises since there are a few prior implications that properly guides individuals to a concrete decision on how to deal with these specific circumstances. There are new challenges that investigators, justices, and other groups face when it relates to a reasonable expectation of privacy and technology.

To begin with, the matters addressed above correlate to the 2018 court case *Carpenter v. United States*. Timothy Carpenter, along with several other men, was connected to several robberies in the Detroit area around 2011. Law enforcement was able to apprehend a few of the perpetrators and manage to obtain a confession from one of them about their elaborate operation of robberies across two states; he professed that his group was able to commit several robberies in Michigan and Ohio. The perpetrator cooperated with law enforcement and offered the names and phone numbers of his co-conspirators. After the FBI gathered information, prosecutors were able to pinpoint who committed the robberies by obtaining cell records through court orders. Among those that were identified as suspects of the felony, Timothy Carpenter was one of them. The court orders granted law enforcement and prosecutors the authority to have Carpenter’s wireless carriers divulge information on incoming and outgoing phone calls during the period that the string of robberies occurred. The cell site location information (CSLI) helped to further their case against Carpenter. This type of technology has the ability to monitor a time-stamped record of a cell site while cell phones tap the wireless network. The FBI was able to obtain data that located the area he was in while the robberies occurred. During Carpenter’s trial at the District Court, he disputed that the government did not have the right to his records, and it infringed upon the rights that were established in the Fourth Amendment since a warrant was not involved. The District Court rejected his argument allowing CSLI as evidence. This data showcased that Carpenter’s cell phone was located near several robberies that he was suspected of committing. Christopher Hess offered expert testimony about CSLI too. As a result of the evidence collected by the FBI, Carpenter was found guilty of being the mastermind behind the robberies and was sent to prison for one hundred years. Carpenter’s argument was also denied at the Sixth Court of Appeals since they claimed that he did not have the reasonable expectation of privacy because the CSLI was distributed amongst his wireless carriers; they considered CSLI to be like business data, which is not protected under the Fourth Amendment. The Supreme court’s decision deviated from both the District Court and Sixth Court of Appeals decision. The Supreme Court decided that the government agencies involved in the investigation violated the Fourth Amendment’s right in opposition to unwarranted search and seizures when they obtained his CSLI. Therefore, I agree with the Supreme Court’s majority opinion that a warrant must be issued when retrieving data for longer than the allotted time that locates individuals through their cell phones. Although gathering it is important to gather concrete evidence that can assist in convicting perpetrators, law enforcement and other government agencies do not have the right to encroach on peoples’ right to privacy. If law enforcement produces a warrant, there will be little to no dispute over the validity of the search. It helps law enforcement investigate effectively. It does not only protect people, but it can also protect law enforcement and other government agencies.

Consequently, both the Fourth Amendment and Stored Communications Act related to *Carpenter v. United States*. The Fourth Amendment was meant to protect people from arbitrary search and seizures. Carpenter claimed that the government seizing his stored data from service providers was a violation of the Fourth Amendment since they did not have a warrant to obtain that information. The Stored Communications Act acknowledged privacy rights for electronic data gathered by service providers of electronic communication. The act tries to prevent unauthorized access to a subscriber’s sensitive information and prevent service providers from abusing their authority and offer their subscriber’s sensitive information to an unauthorized third party. It also specifies that government agencies have the authority to obtain a subscriber’s stored data if a court order is shown to service providers. This act gave prosecutors the power to take custody of Carpenter’s cell phone records on the basis that the information stored on his cell phone was imperative for the case against him since they had a court order to receive such material. The key difference between the two regarding privacy is that the Stored Communications Act provides fewer privacy protections to information that is stored remotely or by a third party the Fourth Amendment entails that the government must obtain a warrant that specifies what they are searching for and seizing.

Next, several Supreme Court cases were considered with the majority opinion. In *Katz v. United States*, Katz was broadcasting gambling information on the telephone to his clients across several states. To catch his criminal behavior, the FBI utilized eavesdropping devices on the telephone that Katz frequently used. Katz was eventually convicted and wanted to dispute over the use of recordings as evidence during his trial. The Supreme Court determined that the Fourth Amendment protected Katz’s correspondence with others, but people’s physical movements are not protected under the amendment. Regarding Carpenter’s case, the Supreme Court that monitoring Carpenter’s movements through CSLI is a violation of the Fourth Amendment. The Supreme Court claimed that people deserve privacy regardless of if they’re at their home or walking in the street. Carpenter had a fair expectation of privacy regarding that problem. In the case *Smith v. Maryland*, law enforcement was investigating a robbery and menacing calls from an unknown suspect, they figured out his identity by obtaining a pen register from a phone company and found the victim’s home number was dialed by Smith. Smith also argued over the verdict and claimed that law enforcement did not have permission to access his pen register because there was not a warrant. The Supreme Court held that phone numbers are not protected under the Fourth Amendment because phone numbers are willingly given to third parties. Although the Supreme Court agreed that information shared by third parties is not a violation of the Fourth Amendment, the majority clarifies that since CSLI brings about new challenges it is difficult to determine a concrete principle to mitigate it regarding privacy protections. While discussing Carpenter’s case the majority agreed that long term surveillance of people. was unconstitutional. In *U.S. v. Miller*, Miller was found guilty of not paying his liquor tax for his distilling equipment. To convict, Miller law enforcement subpoenaed his accounts from his banks. He also claimed that looking through his bank statements was a violation of the Fourth Amendment. The Supreme Court countered his claim and held that his account was not protected under the Fourth Amendment. Regarding Carpenter’s court case, utilizing a court order or subpoena to obtain information from a third party such as service providers disregards Fourth Amendment protections. In *Riley v. California*, Riley was pulled over, and law enforcement found out that Riley’s license was suspended and took custody over his car. Before his vehicle got confiscated, police had to search his car. While conducting their search law enforcement found firearms. They also managed to connect him to a shooting and other gang activity while searching through his phone and running tests. Prior to the trial, Riley tried to prevent the information from his phone to be used as evidence. Although Riley was convicted, the Supreme Court acknowledged that Riley’s Fourth Amendment right was violated because law enforcement did not have the authority to search through his phone without a warrant since it did not compromise the safety of law enforcement. This case relates to Carpenter’s case because the majority agreed that law enforcement only obtained a court order rather than a warrant to gather evidence from his service providers. Also, that law enforcement did not have sufficient reasons to investigate warrantless.

Thus, law enforcement now needs to attain a search warrant when monitoring a person’s location with unconventional technology like CSLI. Obtaining a subscriber’s CSLI is regarded as a search, and law enforcement and other governmental agencies must provide a warrant that substantiates a reason to acquire the data; Neither a court order nor subpoena will suffice. As I stated above, the majority in the Supreme Court case determined that obtaining CSLI from a third party for a certain amount of time without a warrant is a violation of the Fourth Amendment because people have a reasonable belief of privacy regarding that information.

Works Cited

Packard, Ashley. *Digital Media Law*. 2nd ed., John Wiley & Sons, Inc., 2013.

"Carpenter v. United States." *Oyez,* www.oyez.org/cases/2017/16-402. Accessed 13 Oct. 2021.

"Katz v. United States." *Oyez,* www.oyez.org/cases/1967/35. Accessed 14 Oct. 2021.

"United States v. Miller." *Oyez,* [www.oyez.org/cases/1975/74-1179. Accessed 15 Oct. 2021](http://www.oyez.org/cases/1975/74-1179.%20Accessed%2015%20Oct.%202021).

"Riley v. California." *Oyez,* www.oyez.org/cases/2013/13-132. Accessed 15 Oct. 2021.