Supreme Court to hear Carpenter v. United States, a case about privacy in the digital age

Trévon Austin
29 November 2017

The US Supreme Court is scheduled to begin hearings today on *Carpenter v. United States*, a case which holds significant implications for democratic rights. The case, which raises questions on whether or not citizens have reasonable expectations of privacy in the digital age, is expected to be the most important Fourth Amendment case in a generation.

In April 2011, police arrested four men connected to a series of armed robberies. One of the men involved confessed to the crimes and gave officers his cell phone number and the numbers of others involved in the robberies.

The FBI used the numbers of the other participants to apply for three orders from magistrate judges to obtain "transactional records" for each of the phone numbers, which the judges granted under the Stored Communications Act.

The act states the government may request the disclosure of certain telecommunications records when "specific and articulable facts show 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."

In this case, the records obtained by the FBI included the date and time of calls, and the approximate location where calls began and ended based on information from cell towers. All of the information used was gathered without an issue of a warrant.

For a total of 127 days, historical cell-site information (CSLI) was collected regarding phones used by defendant Timothy Carpenter, who had been named by an accomplice as the mastermind of a string of nine commercial burglaries committed in and around Detroit.

Every time a cell phone signals its provider, to send a text message, to start or end a call, or just to get a notification, it sends a time-stamped piece of information, including its location with the nearest cell tower. This data, CSLI, is not accurate like GPS, but can be used to calculate a person's location within a two-mile radius. The evidence gathered in this case was nearly eight years ago and newer technology makes tracking even more accurate.

Central to *Carpenter* and the implications for privacy law is how the government's collection and use of CSLI data holds up against the Fourth Amendment. The Fourth Amendment guarantees citizens security against "unreasonable searches and seizures" and states "no warrants shall issue, but upon probable cause."

In the past, the Federal courts have had a mixed record of upholding and diminishing privacy law. In *United States v. Jones*, one of the most recent and similar cases dealing with the Fourth Amendment, the Supreme Court upheld protections against unreasonable searches and seizures.

In 2005, Antoine Jones was arrested for drug possession after police attached a tracker to Jones' vehicle without judicial approval or a warrant, and followed him for a month. In a 9-0 decision, the Supreme Court held that the installation of a GPS tracking device on Jones' vehicle, without a warrant, constituted an unlawful search under the Fourth Amendment.

In a concurring opinion, Justice Sonia Sotomayor went further to say it may "be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."

However, *Carpenter* presents a situation wherein the Supreme Court's decision may differ from previous ones.

The center of the dispute is the "third-party doctrine," which holds that government access to "voluntary information" given to private businesses, such as banks and cell phone companies, does not constitute a search under the Fourth Amendment, and is therefore constitutional.

The third-party doctrine dates to *United States v. Miller* (1976) and *Smith v. Maryland* (1979), in which the Court affirmed that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."

Technology experts that have filed amicus curiae briefs in *Carpenter* argue that the third-party doctrine was reasonable in the 1970s when telecommunications were not as integrated into citizens' daily lives and the government's ability to access information was not as established but no longer comports with how electronic communications are used today.

Nathan Freed Wessler of the American Civil Liberties Union aims to challenge the collection of CSLI. The ability for authorities to track individuals this way "really changes the game and threatens to upend our expectation of privacy in the digital age," he told NPR.

This case involves more than simply observing a suspect "and never before in the history of this country has the government had the power to press rewind on someone's life and chart out where they were going over the course of four months," Wessler added.

As technology continues to become heavily integrated in daily life, individuals reveal great amounts of information about themselves simply by performing necessary and perfunctory daily tasks. The scope and importance of the internet in day-to-day life make it virtually impossible to not give up "voluntary information" to businesses and corporations.

However, arguments in favor of the US government in this case hold that gathering CSLI without a warrant may not be a violation of the Fourth Amendment. Proponents hold that the data collected in *Carpenter* does not involve "real time" location tracking or the use of GPS data, such as was used in *Jones*.

Professor Orin Kerr, who filed an amicus curiae brief, told NPR that tracking an individual's movements in public is not a new concept. For example, the police may tail a suspect or check on his alibi. Police are only required to procure a warrant when they search a suspect's private property or person. Kerr argued that the CSLI records obtained in the case "are basically the network equivalent of public observation that traditionally would not be protected" by a warrant requirement.

Furthermore, in *United States v. Graham* (2012) the Maryland District Court held that CSLI is not protected under the Fourth Amendment, finding that "information voluntarily disclosed to a third-party ceases to enjoy Fourth Amendment protection" because that information no longer belongs to the consumer, but to the telecommunications company that is providing a service.

In the digital age, individuals should expect to have privacy when daily life depends on interactions with technology and the use of the internet. However, similar to the decision in which the web hosting company DreamHost was forced to hand over information to the government, *Carpenter* could set a precedent that provides a serious basis for the government to freely access personal information and extend its far-reaching domestic spying apparatus.