Forbes

A Guy Who Stole Phones From RadioShack Could Be The Next Face of Digital Privacy

Rebecca Heilweil

June 20, 2018

Timothy Carpenter probably wasn't thinking about Ruth Bader Ginsburg or Clarence Thomas when he—along with several armed co-conspirators—stole cell-phones from RadioShack and T-Mobile stores in Ohio and Michigan.

But now, Carpenter is at the center of the most pivotal Fourth Amendment Supreme Court case in years. The justices are weighing whether law enforcement's warrantless access to months of cell tower location data, used to study Carpenter's movements, is unconstitutional.

The decision could be released as early as Thursday.

The case focuses on two key questions regarding digital privacy: what constitutes voluntarily submitting your information to a third-party, and when does law enforcement obtaining that information require a warrant?

The justices—all of whom are over 50—are sometimes criticized for misunderstanding technology. Justice Anthony Kennedy once referred to programmers as a "computer group of people." Yet the Court has also acknowledged that the Constitution, on its own, cannot keep up with the speed of technological advancement. Critics especially worry that Supreme Court's traditional approach toward these types of Fourth Amendment questions isn't built for a post-Cambridge Analytica world, where users regularly and often unknowingly share their personal information.

Privacy advocates believe that a Supreme Court decision in favor of the government could make citizens even more vulnerable to surveillance by law enforcement.

In *Carpenter v. United States*, law enforcement obtained Carpenter's location records through a court order, which, unlike a warrant, does not require probable cause. This strategy isn't unusual. Cell service providers like Verizon and AT&T respond to tens of thousands of these types of law enforcement requests each year. Collected by hundreds of thousands of cell towers across the country, cell phone location records can be used to create a detailed profile of where the phone's user has traveled. The devices regularly connect to cell-towers hundreds of times a day.

The government contends that Carpenter had "no legitimate expectation of privacy," as the information was collected by a third-party (Carpenter's cell phone service provider). The

government argues that “cell-phone users are aware that they must be in a tower’s coverage area to use their phones, and they must understand that their provider knows the location of its equipment and may make records.”

The “third-party doctrine”—that sharing information with third-parties generally annuls someone’s reasonable expectation of privacy—was established decades ago in *United States v. Miller* (1976) and *Smith v. Maryland* (1979).

The American Civil Liberties Union, which is representing Carpenter, contends that law enforcement's obtention of its client's data was an unconstitutional "search" of his private information over a long period of time.

"Unlike a phone number entered into a phone to connect a call or a check passed into commerce to be drawn on an account, cell phone location data does not necessarily involve any voluntary act on the part of users," Carpenter's defense argues. "The data is created whenever mobile devices receive a call, text message, or data connection, requiring no activity of a user whatsoever."

Carpenter's case has the support of a number of non-profits, including the Cato Institute, a libertarian think-tank, the Electronic Frontier Foundation, a digital rights group, and the Reporters Committee for Freedom of the Press.

Ilya Shapiro, an attorney and fellow at the Cato Institute says his group has “been pushing the idea of re-framing the test the Court should apply in thinking about these kinds of questions.”

Shapiro argues that the legal construct of the reasonable expectation of privacy, as well as the third-party doctrine, do not “transfer well” for legal questions created by new technologies. “In the digital world, [the Fourth Amendment] means more than physical types of protection,” he adds. “You maintain a property interest, in addition to a privacy interest, in all sorts of digital materials.”

Justice Sonia Sotomayor has also questioned the utility of the third-party doctrine, writing in 2012 that the framework “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.”

A decision in favor of the government, Shapiro says, could incentivize the development of encryption and protection technologies that would block cell providers from accessing their own users’ information.

Jennifer Lynch, an attorney at the Electronic Frontier Foundation, argues that location information is protected by the Fourth Amendment and requires a warrant. While investigating Carpenter, law enforcement was able to access seven months worth of location records, she says, “a vast amount of data that reveals a vast amount of personal and private information."

Lynch says that the third-party doctrine is irrelevant. "Let’s say you rent an apartment and your landlord has access to your apartment. Just because the landlord has access to your apartment doesn’t mean that they can give access to law enforcement.”

If the Supreme Court decides against Carpenter, Lynch says the government "could use location tracking to track anyone it wants."

“One of the things that is threatened when the government has a surveillance apparatus is that allows it to track people without their knowledge. It threatens democracy,” Lynch adds. “If people know they’re being surveilled by the government, it chills their ability to speak freely about things.”