Supreme Court Extends Fourth Amendment Protections To Include Mobile Phone Carrier Location Data

Andrew Feinberg

June 22, 2018

WASHINGTON, June 22, 2018 — People living, working, or traveling in the United States gained a bit more privacy Friday after the Supreme Court found that police must obtain a search warrant before asking wireless carriers to turn over some types records which reveal a mobile phone's location history.

In the case of *Carpenter v. Sessions*, a five-justice majority found that prosecutors should have obtained a judge's consent before asking two wireless carriers to turn over petitioner Timothy Carpenter's cellular site location information.

The information included 12,898 location points documenting his movements over the course of 127 days. Instead of using theprocedures laid out under the Stored Communications Act - which require a lower burden of proof - the high court required the probable cause standard needed for a search warrant.

Writing for himself and the four justices considered to be the court's liberal wing — Ruth Bader Ginsberg, Stephen Breyer, Sonya Sotomayor and Elena Kagen, Chief Justice John Roberts opined that the "unique nature" of CSLI differentiates it from other kinds of stored data held by a phone company.

That made it subject to the protections of the Fourth Amendment.

A higher expectation of privacy

"Whether the Government employs its own surveillance technology as in Jones or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. The location information obtained from Carpenter's wireless carriers was the product of a search," he wrote.

Citing *United States v. Jones.*, in which the court ruled that a search warrant is needed to place a GPS tracking device on a suspect's vehicle, Roberts said Carpenter had a reasonable expectation of privacy when it came to records of his movements, and allowing the government to access those records without a warrant "contravenes that expectation" despite the fact that his phone carrier — not the police — collected the information for commercial purposes.

Roberts also noted that the collection of a person's mobile phone location records presents "even greater privacy concerns" than tracking a vehicle because people "compulsively carry cell phones with them all the time."

"A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales," he explained, comparing the use of phone location records to having GPS ankle monitor which can go back in time attached to any person it wishes to track.

Conservative dissenters found fault with Roberts' reasoning

Dissenting justices, however, found fault with the majority's reasoning for a number of reasons.

Justice Anthony Kennedy, a Reagan appointee who is often a deciding swing vote in 5-4 decisions, admonished the majority for an "unnecessary and incorrect" departure from the precedents and principles of the Fourth Amendment that would hinder law enforcement with "undue restrictions" on the ability to investigate violent crimes.

Writing for himself and Justices Clarence Thomas and Samuel Alito, Kennedy explained that cell site location were no different from any other records which are subject to subpoena, adding that mobile phone service subscribers should have no expectation of privacy in them because of their imprecise nature.

But the opinion was also joined by the court's newest member, Justice Neil Gorsuch, who argued that protecting Americans' privacy would be easier if the court deep-sixed the current patchwork of case law.

Instead of continuing with an array of laws governing the government's ability to track people with GPS devices, or by accessing records like CSLI, Gorsuch argued in favor of an approach guided by the specific protections laid out in the Fourth Amendment.

Civil libertarians pleased with the outcome

Despite the court's clear divisions over this particular case, civil libertarians and privacy advocates hailed the ruling as a victory for Americans' right to privacy while recognizing the need to update laws governing law enforcement access to personal information in the digital age.

American Civil Liberties Union attorney Nathan Freed Wessler, who represented Carpenter before the Supreme Court, called the decision "a groundbreaking victory for Americans' privacy rights in the digital age."

"The government can no longer claim that the mere act of using technology eliminates the Fourth Amendment's protections. Today's decision rightly recognizes the need to protect the

highly sensitive location data from our cell phones, but it also provides a path forward for safeguarding other sensitive digital information in future cases — from our emails, smart home appliances, and technology that is yet to be invented."

Sen. Ed Markey, D-Mass., praised the court's decision as an appropriate 21st century update to fourth amendment jurisprudence.

"Where we go or where we have been is sensitive information that should only be revealed to law enforcement with a warrant. The Court's decision takes a big step forward for privacy by saying the government can't track a person's past movements through the records of their cell phone signal without probable cause," said Markey, a member of the Senate Commerce Committee.

"Police need a warrant to search an individual's home, and that will now be the standard for mobile phone location records, as well. We need to continue to update our laws to protect the privacy of Americans in this increasingly digital world," he said.

However, Markey also acknowledged the need for Congress to update privacy laws for the digital world.

Not all digital data is created equal

Julian Sanchez, a Cato Institute scholar who has written extensively the intersection of technology, privacy, and civil liberties, told *BroadbandBreakfast* that one positive takeaway from the *Carpenter* decision is "the idea that not all data is not created equal.

"The fact that some types of information are obtainable from third parties from a subpoena doesn't mean that every conceivable kind of data — no matter how intimate — is subject to the same rule," Sanchez said when reached by phone on Friday. "But they don't say a whole lot about what, other than location, that might be."

Sanchez cautioned that the narrow nature of the ruling, in which the court took pains to distinguish CSLI as subject to the Fourth Amendment's protections while still leaving open the possibility that other kinds of data that might reveal location information deserved similar treatment, meant the court did not give much guidance as to what else might be protected.

"There's a huge quantity of information that third parties retain that is arguable sensitive or intimate or revealing in various ways," he said, adding that because of a differences between the protections provided by the Stored Communications Act and the Electronic Communications Privacy Act, the same kinds of data can be treated differently by different companies when it comes to allowing the government to access it without a warrant.

For example, Sanchez said differences between the SCA and ECPA mean that if GPS data collected by Google is treated as communications between Google and the owner of a mobile phone, it would not necessarily be given the same protections *Carpenter* now gives data held by wireless service providers.

Resolving the "incoherence" between the SCA and ECPA should be a priority for lawmakers, Sanchez said.

"One thing Congress could do is step up and say what types of data might be subject to stronger protections, and not just assume that that the only relevant distinction is between communications content and everything else, which is how the law currently treats it."

Sen. Leahy argues for a new legal paradigm on privacy

Sanchez's sentiments were echoed in a statement by the ranking member of the Senate Judiciary Committee, Sen. Patrick Leahy, D-Vt., who said Friday's ruling "perfectly illustrates that old legal constructions, like the third-party doctrine, struggle to keep up with our 'seismic shifts in digital technology.'

"As more and more of our sensitive information is held by third parties, this decision is a step forward in ensuring that our most private information — our communications, our photos, our financial and medical records, our every location — receives the Fourth Amendment protection it deserves," said Leahy.

Leahy cautioned that Congress "must not rely on the courts to modernize our antiquated privacy laws" while noting that a bill he co-sponsored with Sen. Mike Lee, R-Utah., would require police to obtain a warrant for the exact type of data at issue in *Carpenter*, and would close "other major loopholes in protecting our Fourth Amendment privacy rights, like requiring a warrant for electronic content."

"Congress must not abdicate its own responsibilities as technology advances, and it should quickly take up our legislation to accomplish these key reforms."