Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# The Privacy Fight For Digital Data Warrants Is Just Starting

By **Ben Kochman**

*Law360 (September 14, 2018, 10:32 PM EDT)* -- Lower courts are already grappling with the U.S. Supreme Court's June ruling in U.S. v. Carpenter telling authorities to get a warrant for cellphone location data, which privacy lawyers say is just the tip of the iceberg as disputes loom about other types of digital data that can reveal intimate details about someone's life.

Two cases pending at the highest state courts in Massachusetts and Maine raise the question of whether the Fourth Amendment protections the high court in June granted to data that traced convicted bank robber Timothy Carpenter's past movements through his cellphone apply to tracking someone's movements in real time.

And despite the high court's insistence that its split decision was "a narrow one," privacy advocates and ex-prosecutors say it won't be a stretch to see lower courts try to apply the Carpenter ruling's logic to other sensitive data sets like online browsing history that both are indispensable to investigators and spawn privacy concerns.

"Given the reasoning of the decision, one would expect to see challenges when law enforcement, without obtaining a warrant, seeks digitally collected data that in the aggregate can draw a picture of not only location but also other personal or private details of a person's life," said Larry Sommerfeld, a former federal cybercrimes prosecutor in the Northern District of Georgia and now a partner at Alston & Bird LLP.

The high court's ruling in Carpenter chipped away at a legal principle known as the third-party doctrine, which in cases dating back to the 1970s has allowed the government to warrantlessly access data that consumers "voluntarily" handed over to third parties like banks or credit card companies. In Carpenter's case, the FBI obtained what's called a 2703(d) order under the Stored Communications Act, which requires authorities to show that the requested data is "relevant and material to an ongoing investigation" — a lower threshold than the probable cause required for a warrant.

In his decision for the majority, Chief Justice John Roberts wrote that cell-site data — which pinpoints someone's location when that person's phone connects to a nearby cell tower — is different than other types of information held by third parties. Cellphones are indispensable to participating in modern life, Justice Roberts wrote, adding that a cellphone logs cell-site data that can be used for tracking purposes "by dint of its operation, without any affirmative act on the part of the user beyond powering up."

In the two New England cases being considered this month, Commonwealth v. Almonor in Massachusetts and State v. O'Donnell in Maine, privacy advocates with the American Civil Liberties Union and Electronic Frontier Foundation are citing Carpenter in calling for the courts to establish a clear warrant requirement for cellphone location data used to track down suspects in real time, rather than the historical data addressed in Carpenter.

In the Almonor case, Massachusetts prosecutors say that officers should not have had to get a warrant before asking Sprint for location data that helped them pinpoint a murder suspect in a private home. Authorities say the officers had exigent circumstances — namely, that they were trying to find an on-the-loose murder suspect — that make it unreasonable to expect them to have obtained a warrant.

But in a March brief, months before the Carpenter decision came out, the authorities also argued that police only need to ask for a warrant when they are asking for more than six hours of total data, citing a 2014 Massachusetts state high court ruling in a case called Commonwealth v. Augustine. Privacy advocates say that six-hour limit for warrantless surveillance is now unconstitutional in the wake of Carpenter, in which the justices said the government should "generally" obtain a warrant before acquiring such records.

In the Maine case, police asked Verizon to "ping" the phones of two burglary suspects, who they then located in a Motel 6. A trial court, citing the third-party doctrine, ruled that the request for real-time location data was not a Fourth Amendment protected search — an idea privacy advocates say the high court rejected in Carpenter.

"Aspects of real-time tracking are even more invasive than historical tracking," Andrew Crocker, an EFF staff attorney, told Law360. "It seems to us like the reasoning of the Supreme Court should apply, if not in the same way, then potentially more so for real-time searches."

Courts are likely to rule with the government if authorities can reasonably claim a public safety purpose for pinging a suspect's phone, such as if the suspect is about to commit a crime or destroy evidence, said Sarah Hall, senior counsel at Thompson Hine LLP and a former federal prosecutor.

"If it's part of a generic investigative activity, then possibly these courts will view it in a more Carpenter-esque way," she added.

Judges in the New England cases could decide that the warrantless searches are still valid because they were made in good faith before Carpenter, which is what federal appeals courts in the Second and Seventh Circuits **ruled** in August when asked to consider overturning convictions made with evidence obtained in warrantless cellphone location data before the high court's ruling.

In the Massachusetts case, police had not even "contemplated procuring a search warrant for the cell site location information because they did not believe they were required to," according the government's brief.

In Timothy Carpenter's case, the government obtained records spanning 127 days from MetroPCS and two days from Sprint, a total of 12,898 location data points that chronicled his movements and placed him near the scene of four robberies in Michigan and Ohio.

But it's unclear from the court's ruling whether law enforcement would be required to get a warrant for smaller, arguably less intrusive blocks of historical location data, said Jed Davis, a Day Pitney LLP partner

and former federal cybercrimes prosecutor in the Eastern District of New York.

Authorities may decide to press the issue — asking for records for a single hour during business hours when a suspect is in a public place, for example — to see where lower courts draw that line, he said. The issue is particularly crucial because of the importance of cellphone location orders as a "building block to criminal investigations in a mobile world," Davis said.

"There will be instances where law enforcement is going to test how far this applies," he said.

Privacy hawks say they plan to apply Carpenter's logic to future cases where questions arise about whether Fourth Amendment protections apply to other sets of data held by third parties. Governments are likely to be challenged over whether they can warrantlessly obtain data that provides authorities with sensitive and potentially invasive information, such as medical information gleaned from a fitness app or webpages someone browses online.

"Carpenter set the model for what courts looking at this sort of electronic surveillance will do, and is the strongest signal so far that the government can't just rely on the third-party doctrine," said Crocker. "The Supreme Court has been very protective of information which could be invasive in someone's home, and Carpenter provides more support for the idea that that type of information should be protected."

Authorities are particularly likely to fight back against attempts to curb their access to browsing history, which is commonly used in criminal cases, said Hall.

"If defense attorneys begin to challenge law enforcement's ability to get browsing history without a warrant, they are going to have a massive fight on their hands," she said.

The results of the inevitable legal battles about the scope of the third-party doctrine may end up confusing both law enforcement and privacy advocates, if lower courts yield inconsistent results, said Davis.

"It remains to be seen whether the third-party-doctrine survives, and whether the court's characterization of location data as different from other forms of [third-party-held] information survives," he added.

--Editing by Pamela Wilkinson and Kelly Duncan.