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

Location Privacy Warrant Lines Still Murky After Carpenter

By **Allison Grande**

Law360 (August 19, 2019, 8:52 PM EDT) -- District courts have been reluctant to require warrants for access to digital records beyond the historical cellphone location data covered by the U.S. Supreme Court's Carpenter decision, but appellate courts may end up flipping the script as criminal defendants and service providers continue to fight back.

The high court ruled last June in Carpenter that records held by third-party wireless carriers about the location of cell towers used to route calls to and from cellphones are entitled to heightened privacy protections and require a warrant to obtain. However, the court left open whether the requirement applies to other categories of sensitive digital data, such as real-time cellphone records, internet browsing histories, toll transactions and smart meter usage.

Criminal defendants and the service providers that hold these records are pushing for the Fourth Amendment principles articulated by the Supreme Court to apply beyond historical location records. But district courts during the past year have largely been hesitant to go beyond the narrow confines of Carpenter, so eyes are turning to appellate courts to see if they will embrace a similar approach.

"What we've seen in the first year is a lot of district courts sticking to the facts of Carpenter in interpreting it more narrowly than some of us thought they would," said Ed McAndrew, a former federal cybercrime prosecutor and current cybersecurity and litigation partner at DLA Piper. "This next year is going to be really important as appellate courts weigh in on Carpenter's application to these other types of digital data."

The Carpenter decision chipped away at the third-party doctrine, a 1970s-era legal principle that states people who voluntarily give their personal information to banks, phone companies or internet service providers can't reasonably expect that information to stay private.

The ruling was the latest high court decision to make clear that older search doctrines "can't just be mechanically extended to new digital age technologies," said Nathan Freed Wessler of the American Civil Liberties Union, who argued the case on behalf of Timothy Carpenter at the high court.

"If the government had won in Carpenter, it would have thrown open a dizzying array of our most sensitive and personal information to law enforcement in an age where it's impossible to be a human being without leaving incredible trails of data reflecting the most sensitive parts of our lives, not just on our own devices but with the companies we interact with," Wessler told Law360.

In the 14 months since Carpenter was handed down, the ACLU has jumped into litigation surrounding law enforcement's access to sensitive information such as the detailed data collected by modern cars, prescription records and the contents of electronic devices seized at the border.

The group plans to continue to watch for emerging issues surrounding the seizure of data gathered by new technologies such as home devices and smartwatches to ensure that lower courts "heed the high court's call and extend the lessons of Carpenter to other contexts," Wessler said.

"There are dozens of applications of the third-party doctrine that have to be dealt with by courts in the coming years," he said. "It's a slow process, but what the Supreme Court has made clear is that the third-party doctrine is not an on-off switch and the mere fact that your data is held by a company doesn't eliminate your Fourth Amendment rights."

While the high court didn't establish a test for what types of data seizures trigger these warrant protections, the justices did offer several factors for courts to consider when deciding whether Carpenter applies, Wessler said. Those include how revealing the data at hand is, how much of it was collected and for how long, whether it was voluntarily shared by the user and whether law enforcement could have built its case another way.

"The Carpenter decision was groundbreaking in terms of its recalibration of the third-party doctrine for the digital age, but its ultimate effect and sweep is still to be determined because courts are really grappling with different types of digital data and the privacy implications of government seizures and uses of that data," McAndrew said.

As new technologies continue to emerge, criminal defendants like Carpenter — who challenged the government's warrantless collection of 127 days of historical cellphone location records that were ultimately used to help convict him of six robberies in Michigan and Ohio — will no doubt continue to argue that the Supreme Court's reasoning applies to a range of other types of digital data, according to Harry Sandick, a partner at Patterson Belknap Webb & Tyler LLPand former federal prosecutor in the Southern District of New York.

"The biggest open question will be, where does the law go from here?" Sandick said.

Pressure to expand Carpenter's reasoning beyond historical cell tower records isn't just coming from inside the courtroom. Service providers that hold this sensitive information are already pushing law enforcement to obtain warrants for a wider range of personal information and will likely hold strong in this stance, according to attorneys.

"Tech companies are more aware of the significance and importance of privacy to their customers and subscribers, so they're taking more measures and steps to ensure the privacy of their customers and pushing back on demands by the government for the data in their possession by trying, like the defense bar, to have more things afforded protections of a search warrant rather than a subpoena," said Hanley Chew of Fenwick & West LLP, a former federal prosecutor in the Northern District of California.

Mark Krotoski, a partner and co-leader of Morgan Lewis & Bockius LLP's privacy and cybersecurity practice, noted that companies are not only establishing practices to comply with Carpenter with requests for cell site location records but are also mindful that Carpenter may soon be expanded to cover other types of location information.

"Carpenter is definitely an invitation for more challenges in this area, given how many issues the decision left open," Krotoski said.

As service providers and defendants continue to mount these fights, law enforcement agencies are pushing to preserve their ability to obtain vital about alleged crimes with a subpoena rather than a warrant, which has a higher standard for probable cause, attorneys say.

Law enforcement has limited the spread of Carpenter in the lower courts, but there's no guarantee that appellate courts will yield the same results.

In one of the few warrant cases to reach an appellate court, the Seventh Circuit ruled last August that the Fourth Amendment protects energy-consumption data gathered by smart meters because these devices reveal intimate details about what's going on inside a home. However, the court declined to halt the challenged collection of this data by the city of Naperville, Illinois, finding that the government's benefits of using the meters make the search reasonable.

Advocacy groups including the ACLU and Electronic Frontier Foundation applauded the decision, which they noted was the first to address whether the Fourth Amendment protections laid out in Carpenter apply to smart meter data and went against earlier rulings that refused to find that individuals have a right to privacy in monthly energy usage readings from traditional, analog energy meters.

The appellate court also noted that its analysis would have been different if the contested search were conducted with "prosecutorial intent," if the search were conducted by law enforcement instead of the city's public utility, or if the data was more easily accessible to law enforcement or other city officials outside the utility, EFF noted. This leaves open significant questions about how far appellate courts are willing to go to limit these type of searches when they involve law enforcement personnel, attorneys say.

"If appellate courts start reversing and throwing out convictions due to digital evidence that was collected without a warrant, we'll have a much clearer picture of the real implications of Carpenter," McAndrew said.

Such rulings could have a sweeping impact on criminal investigations and prosecutions, as law enforcement commonly uses a broad range of records maintained by third parties to build probable cause for a warrant.

Examples have already begun to emerge in the narrow context of the historical location records covered by Carpenter.

McAndrew pointed to the case of Benjamin Rauf, who was charged in Delaware with the 2015 murder of his former law school classmate.

Rauf moved to challenge law enforcement's warrantless pre-Carpenter seizure of his cellphone location data, which put him in the area at the time of the shooting. While several federal appellate courts have allowed prosecutors to use cell site data obtained before the Supreme Court's ruling — including the Sixth Circuit on remand in the Carpenter dispute — Delaware has not recognized this good-faith exception to the Fourth Amendment.

Facing uncertainty about whether this evidence would be excluded in the absence of an argument that officers were acting in good faith when they collected this data, prosecutors agreed to offer Rauf — who was facing the possibility of life in prison — a 15-year sentence in exchange for his guilty plea.

"That's probably the starkest example that I know of with respect to the effect of Carpenter in altering the course of an investigation, prosecution and sentence," McAndrew said.

The Carpenter decision may also prompt more states and possibly the federal government to enact laws cementing the Fourth Amendment principles articulated by the high court.

Utah earlier this year became the first state to require police to obtain a warrant before they can gain access to anyone's electronic data, and experts say they wouldn't be surprised to see more jurisdictions pick up this thread.

"Both courts and legislative bodies have a critical role to play in protecting privacy in the digital age," said Wessler, the ACLU attorney. "After Carpenter, lawmakers have an opportunity to bring clarity more quickly than courts can to what the rules are and when a warrant is required for access to sensitive information."

--Editing by Brian Baresch and Breda Lund.