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

High Court Ruling May Spur Broader Location Privacy Limits

By **Allison Grande**

Law360 (June 22, 2018, 10:46 PM EDT) -- The U.S. Supreme Court's split ruling Friday that historical cellphone location records are entitled to heightened privacy protections not only deals a major blow to law enforcement, but could also jeopardize the way private companies such as Google and Facebook currently use and share sensitive information by giving ammunition to courtroom challenges and policy efforts to rein in these practices, attorneys say.

In a 5-4 ruling that came nearly seven months after oral arguments were held, the high court rejected the federal government's argument that individuals such as petitioner Timothy Carpenter don't have a legitimate expectation of privacy under the Fourth Amendment in the records that third-party wireless carriers compile and maintain of the location of cell towers that are used to route calls to and from cellphones.

"This ruling is among the most important privacy decisions to date from the Supreme Court and really builds momentum in terms of limiting the government's investigative techniques and championing individuals' privacy rights, and has the potential to spill over to lots of different areas both in the courts and in the legislative and regulatory contexts," said Ed McAndrew, a former federal cybercrime prosecutor who now co-chairs the privacy and security group at Ballard Spahr LLP.

The high court's ruling is likely to have the most immediate and obvious impact on federal law enforcement officials, who have typically relied on such historical cell site information to establish a suspect's involvement in a crime and support probable cause for further searches. But the majority's conclusion that individuals have the right to expect that their location data will remain private could spark broader consequences for companies that gather such sensitive information for their personal use, according to attorneys.

"In light of the fact that this is the highest decision so far that has involved the issue of privacy protections for location data, it's definitely possible that the ruling could be cited by consumers to support the argument that private companies should afford greater privacy protections to this type of data," said Hanley Chew, an attorney with Fenwick & West LLP and former federal cybercrime prosecutor.

In a call with reporters Friday, Nathan Freed Wessler of the American Civil Liberties Union, who argued the case on behalf of Carpenter, said while the Fourth Amendment issues raised in the case directly apply only to the federal government, "the really strong and robust recommendation that people have

intense privacy interests in this information may well prove important in other litigation over privacy rights in the private sector."

Service providers such as Facebook and Google are no strangers to class action litigation challenging the ways they use, collect, share and monetize private data such as browsing histories and location data, and attorneys on both sides of the bar said they wouldn't be surprised to see the high court's Carpenter decision cited in these disputes moving forward.

"The court's recognition of an expectation of privacy in consumer location data is a huge victory for those of us who care about privacy," said Ryan D. Andrews, a partner at plaintiffs firm Edelson PC. "We expect that recognition to greatly impact how lower courts view private companies' improper use of private consumer data."

Even though the Fourth Amendment doesn't apply to parties outside the government, there's a real possibility that "courts are going to be a little more rigorous in their scrutiny of access to third-party data in private litigation" in the wake of Carpenter, McAndrew said.

The decision could also lead to movement by policymakers at both the federal and state level, which have been especially active in recent months in light of developments such as the European Union adopting a stringent general data protection regulation, or GDPR, and the revelation that political research firm Cambridge Analytica harvested personal information from 87 million unwitting Facebook users, according to attorneys.

"The facts of the Carpenter case highlight how technology gives today's behemoth technology companies almost unlimited access to intrude into our private lives," said Matthew Prewitt, cybersecurity and data privacy group leader at Schiff Hardin LLP. "The law articulated in the Carpenter decision shows again how profoundly inadequate our existing constitutional law, statutory law and common law are to give the Supreme Court and our lower courts any broad basis to tackle these profoundly important issues."

Since the EU adopted its data protection regulation in May, calls have increased for lawmakers to adopt GDPR-like protections in the U.S. One of the most notable efforts on this front is a proposed California ballot initiative that would give consumers the right to ask businesses what categories of personal information a company collects and how it's being used, and to opt out of further collection.

The Carpenter decision could help spur these efforts forward due to the high court's embrace of more stringent protections for location data, which several attorneys said they viewed as a move toward the heightened data protection principles embraced by the EU.

"Right now, we're seeing a trend toward GDPR-type protections and of reevaluation of our approach to privacy in the U.S., and this decision fits in with that," McAndrew said.

Andrew Pincus, a Mayer Brown LLP partner who helped the Center for Democracy and Technology draft an amicus brief in support of Carpenter, said he could see privacy advocates attempting to use Friday's opinion to inform policymaking when it comes to the collection of location information by non-government entities, as well.

"There's certainly a robust discussion currently about the kinds of information that private companies have about people and how it's used, so the argument could be made that the court's determination

about the sensitivity of this information should be used by policymakers in deciding what rules of the road should be when it comes to the private use of this information," Pincus said.

But Prewitt said that while the Supreme Court's decision at first glance appears to provide a boost to digital privacy advocates, the ruling could end up dealing a "major setback" in their policymaking efforts.

"A different decision might have prompted a broad public reaction that maybe — maybe — could have resulted in meaningful legislative reform or at least a broader grass roots privacy movement," Prewitt said. "This decision instead gives the public the false sense that they enjoy meaningful privacy protections and that they may rest easy because the Supreme Court is protecting them. The reality, however, is that the Fourth Amendment has minimal impact on the privacy rights of most law abiding citizens in their daily lives."

Major tech companies including Apple, Facebook, Google, Microsoft, Twitter and Verizon lodged an amicus brief with the Supreme Court last year advocating for a standard that would require the government to obtain a search warrant before approaching businesses with requests for historical cellphone location records. But the brief was not filed in support of either party, highlighting the precarious line that these service providers need to walk, attorneys say.

On the one hand, the decision "gives them more assurance to be able to say that they are protecting this information and basically make more guarantees to their customers that this information is going to be protected" from law enforcement overreach, Chew said.

But on the other hand, that argument presents "a bit of a double-edged sword," since agreeing that consumers have very broad and constitutional privacy rights in location data could spell trouble for their future ability to collect and generate revenue off that same information.

"While the impact on law enforcement from the ruling is going to be immediate, the potential impact on the private monetization and use of consumer data will raise policy battles that remain to be fought," McAndrew said.

Friday's decision also left several open questions for both the government and companies about exactly which categories of data deserve the Fourth Amendment protections bestowed to historical location data. Keeping in line with the high court's previous decisions in U.S. v. Jones and Riley v. California, which both endorsed similar privacy protections for the narrow categories of GPS tracking data and data stored in cellphones, respectively, Chief Justice John Roberts stressed in his majority opinion that the decision was "narrow" and could not be applied to real-time cellphone location data or other issues not currently before the court.

"While the court's adherence to Jones appears to have carried the day by a narrow 5-4 margin, the four separate dissenting opinions reflect multiple fault-lines on this issue," Jaszczuk PC attorneys Daniel Schlessinger and John Kloecker said in a joint email, adding that Justice Neil Gorsuch's dissent appeared "to be based not as much on an opposition to the originalist approach of the majority, but rather on his view that the decision does not provide adequate guidance for lower courts to follow in determining what breadth of surveillance triggers Fourth Amendment scrutiny."

The lack of clear guidance on how the ruling applies to other kinds of non-content data leaves the door open for further fights — and another potential circuit split that could work its way up to the high court — over whether a broad range of data maintained by third parties, including browsing histories, IP

addresses and emails, should be subject to similar robust privacy protections or should fall under the third-party doctrine. That rule, which was limited but not abolished by the Supreme Court in Friday's ruling, dates to the 1970s and established that individuals don't have a reasonable expectation of privacy in certain records voluntarily shared with third-party service providers.

"The opinion distinguishes and carves out long-standing Supreme Court precedent that records voluntarily provided to third parties were not protected by the Fourth Amendment," said Mark Krotoski, a partner and co-leader of Morgan Lewis & Bockius LLP's privacy and cybersecurity practice. "The question now will be whether the carve-out is limited or may be expanded over time."

Chief Justice John Roberts penned the majority decision, which was joined by Justices Ruth Bader Ginsburg, Stephen Breyer, Sonia Sotomayor and Elena Kagan. Justices Anthony Kennedy, Clarence Thomas, Samuel Alito and Neil Gorsuch all filed dissenting opinions.

Carpenter is represented by Nathan Freed Wessler, Ben Wizner, David D. Cole, Cecillia D. Wang, Daniel S. Korobkin, Michael J. Steinberg and Kary L. Moss of the American Civil Liberties Union Foundation, Harold Gurewitz of Gurewitz & Raben PLC, and Jeffrey L. Fisher of the Stanford Law School Supreme Court Litigation Clinic.

The government is represented by Deputy Solicitor General Michael R. Dreeben of the DOJ.

The case is Carpenter v. U.S., case number 16-402, in the U.S. Supreme Court.

--Editing by Kelly Duncan and Catherine Sum.

Correction: An earlier version of this article misspelled the name of Edelson PC partner Ryan D. Andrews. That error has been corrected.
