Every phone leaves a trail — Supreme Court holds location data is protected by the Fourth Amendment

By Jason McCullough, Esq., and Brandon Moss, Esq., Wiley Rein LLP

JULY 15, 2026

On June 29, 2026, the U.S. Supreme Court issued its long-awaited decision in *Chatrie v. United States*, holding that when law enforcement "accesses historical cell phone" location information from a provider, it conducts a search under the Fourth Amendment. In doing so, the Court significantly extended its 2018 opinion in *Carpenter v. United States*.

In *Carpenter*, the Court held that the government's collection of (as little as seven) days of cell-site location information from a wireless carrier was a search, reasoning that individuals retain a privacy interest in such data because of its "revealing" nature given the "pervasive and insistent" role of cell phones in modern society.

Chatrie extends Fourth Amendment protections to any historical cell phone location information generated by third-party applications on a phone.

"It does not matter if the time period scrutinized was only two hours," the Court explained. It does not matter if the location information was generated by a cell phone application whose function is ride-sharing, weather, fast food, or fitness. Under *Chatrie*, historical location information generated by a cell phone is protected by the Fourth Amendment.

The holding and the majority's opinion is significant for technology companies, telecommunications providers, platform operators, and other entities that collect, retain, or process location data. Law enforcement will need to obtain a warrant to obtain any data that reveals detailed historical location information generated from a phone.

Organizations must carefully evaluate governmental efforts to obtain location-related data without a warrant. And the Court's reasoning suggests that these Fourth Amendment protections may ultimately extend beyond location information to other "revealing" data captured on smartphones and stored in providers' records.

The issues presented in *Chatrie*

Chatrie arises out of a 2019 robbery of a credit union. In its investigation, law enforcement obtained a geofence warrant to identify all devices located at the scene of the crime during its commission. The magistrate-issued search warrant authorized a three-step process.

Chatrie extends Fourth Amendment protections to any historical cell phone location information generated by third-party applications on a phone.

In the first step, the technology company searched the location history for all of its users to identify any accounts that were present in a defined area around the credit union (i.e., a 150-meter radius) during a one-hour window. The technology company produced responsive, anonymized location data to law enforcement.

In the second step, law enforcement analyzed the movements of the anonymized accounts, identified a smaller subset that was of interest, and then requested additional location information (i.e., for a two-hour period and without geographic limitations) for that group.

In the third step, law enforcement analyzed the additional data, identified three accounts of interest, and requested subscriber information for those accounts; the information produced in response identified the Petitioner.

The *Chatrie* cert petition presented two primary issues.

First, did the Petitioner have a reasonable expectation of privacy in two hours of detailed location data stored by a technology provider? If he did not, then no warrant was required. On this question, the Court concluded that users have an expectation of privacy in any quantity of historical location data generated by a smartphone.

Second, did the "reverse location" warrant and three-step process utilized by law enforcement in this instance satisfy

Thomson Reuters is a commercial publisher of content that is general and educational in nature, may not reflect all recent legal developments and may not apply to the specific facts and circumstances of individual transactions and cases. Users should consult with qualified legal counsel before acting on any information published by Thomson Reuters online or in print. Thomson Reuters, its affiliates and their editorial staff are not a law firm, do not represent or advise clients in any matter and are not bound by the professional responsibilities and duties of a legal practitioner. Nothing in this publication should be construed as legal advice or creating an attorney-client relationship. The views expressed in this publication by any contributor are not necessarily those of the publisher.

Thomson Reuters™

the particularity requirement of the Fourth Amendment? This issue was left undecided by the Court, though several of the Justices expressed skepticism about the technique.

The *Chatrie* holding

With Justice Elena Kagan writing, the five-Justice majority concluded that "Location History" data generated by smartphones receives Fourth Amendment protection because it provides an extraordinarily detailed record of an individual's movements. Modern location-history databases allow law enforcement to reconstruct a person's movements with precision, retrospectively, and at scale.

The Court characterized this capability as a "virtual panopticon" that could be used by the government to "scrutinize its citizens' activities" and provide "an intimate window into a person's life." In the majority's view, that concern reflects an emerging Fourth Amendment philosophy reflected in modern decisions: The progress of science and technology should not erode constitutional protections.

Smartphone applications and the services they provide have become a "pervasive" and "indispensable" part of daily life, such that users maintain an expectation of privacy in the location data generated through ordinary use — even when that data is held by third-party providers. Individuals therefore do not forfeit Fourth Amendment protection merely because smartphone functionality and modern applications generate location information stored by third parties. Nor can ordinary smartphone use be treated as voluntary disclosure in the traditional sense contemplated by earlier third-party doctrine cases.

The Court's holding answers the principal question left in *Carpenter*'s wake: Fourth Amendment protection is not limited to prolonged location tracking. Unlike *Carpenter*, which involved at least seven days of historical cell-site location information, *Chatrie* involved approximately two hours of location history.

The Court nevertheless held that Fourth Amendment protection applies even to short periods of location data and rejected the notion that law enforcement enjoys a constitutionally permissible "grace period" during which location information may be obtained without a warrant. In the Court's view, when the Fourth Amendment applies, it applies "regardless of the quality or quantity of information the government obtains."

Practical implications for data holders

For telecommunications carriers, technology companies, application developers, connected vehicle companies, advertising platforms, connected-device providers, and other organizations that maintain location information, the most immediate takeaway is straightforward: Requests for location information generated by smartphones must now be viewed through the lens of *Chatrie*'s constitutional holding. If the government requests location data, they'd better have a warrant.

Law enforcement requests for smartphone-generated data that arrive via subpoenas or similar process, such as an order under 18 U.S.C. § 2703(d), should be scrutinized to determine whether the response would reveal the details of a user's historical location and movement. This includes not only traditional geolocation records, but potentially other categories of information that could be used to reconstruct a person's movements, presence at a location, or travel patterns.

With Justice Elena Kagan writing, the five-Justice majority concluded that "Location History" data generated by smartphones receives Fourth Amendment protection because it provides an extraordinarily detailed record of an individual's movements.

Moreover, as we discuss further below, smartphones generate and collect enormous amounts of personal and revealing data. Future Fourth Amendment challenges to smartphone-generated data may expand beyond location data to other information held by providers that could be seen as revealing "intimate details" of a user's life.

Companies should evaluate both their law enforcement disclosure procedures and their terms of use agreements with end users for fidelity with the *Chatrie* holding. *Chatrie* will loom large and may prove a useful tool in future disputes regarding compelled disclosure of location data.

Geofence warrants survive — for now

Notably, the Supreme Court did not hold that geofence warrants — or even the multi-step reverse warrant at issue in *Chatrie* — are Constitutionally infirm "general" warrants. Instead, the Court expressly left those questions unresolved and remanded them to the 4th U.S. Circuit Court of Appeals for further consideration.

At the same time, concurring opinions reflect concern among some members of the Court about reverse-search warrants, with Justice Ketanji Brown Jackson questioning whether the latter stages of the warrant vested law enforcement with excessive discretion without appropriate judicial oversight.

But the voting alignment in *Chatrie* suggests there may not currently be five votes for the broader proposition that geofence warrants are categorically invalid as modern analogues to the general warrants prohibited by the Fourth Amendment. The Court had the opportunity to adopt that rule and expressly declined to do so.

Looking ahead

While *Chatrie* does not end the debate over geofence warrants, it firmly advances the constitutional framework governing smartphone-generated data held by providers.

©2026 Thomson Reuters

First, it cements as black-letter law that government acquisition of smartphone-generated location information is a Fourth Amendment search requiring constitutional justification.

The Court's holding answers the principal question left in Carpenter's wake: Fourth Amendment protection is not limited to prolonged location tracking.

Second, it underscores the need for companies to review law enforcement process that seeks to obtain location information. Organizations must carefully evaluate governmental efforts to obtain location-related data without a warrant and should consult counsel before responding to requests that could reveal an individual's whereabouts or movements.

Third, companies may seek to evaluate whether other types of data generated through the "pervasive" and "indispensable" use of smartphones provide law enforcement a similar ability to intrude upon the most intimate details of a user's life. While *Chatrie* is limited to location data, the Court's holding was guided by the belief that massive amounts of sensitive data are involuntarily transferred to third-party providers by virtue of the use of a phone. Such other sensitive data was not challenged in *Chatrie*, but the Court's rationale may well extend to other sensitive data in future challenges.

Fourth, *Chatrie* leaves unresolved — but likely accelerates — future litigation over geofence warrants and other reverse-search techniques. Companies processing such warrants should pay particular attention to the breadth of the geographic area covered, the duration of the requested search, the number of individuals likely to be swept into the request, and the discretion afforded to investigators during any narrowing process.

In light of *Chatrie*, providers may wish to reassess when it is appropriate to negotiate, narrow, or challenge geofence and other reverse-search requests.

The Supreme Court has now answered the threshold question: Location data is protected. The next major battleground will be determining when government warrants seeking that information are sufficiently particularized to survive constitutional scrutiny.

About the authors





Jason McCullough (L) is a partner at **Wiley Rein LLP**. He is a former federal prosecutor and represents clients in enforcement actions, internal investigations, litigation, crisis management, and compliance matters. He can be reached at jbmccullough@wiley.law. **Brandon Moss** (R) is a partner at the firm. She defends companies and their executives in complex civil and criminal cases in areas including alleged healthcare and FCA fraud, the FCPA, contract and procurement fraud. She can be reached at bmoss@wiley.law. The authors are based in Washington, D.C.

This article was first published on Reuters Legal News and Westlaw Today on July 15, 2026.

© 2026 Thomson Reuters. This publication was created to provide you with accurate and authoritative information concerning the subject matter covered, however it may not necessarily have been prepared by persons licensed to practice law in a particular jurisdiction. The publisher is not engaged in rendering legal or other professional advice, and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional. For subscription information, please visit legalsolutions.thomsonreuters.com.