SUPREME COURT'S CHATRIE DECISION EXTENDS FOURTH AMENDMENT PROTECTION TO LOCATION DATA, RAISING STAKES FOR DIGITAL PRIVACY AND DATA GOVERNANCE

Date: 8 July 2026

US Policy and Regulatory Alert

By: Sanjeev Bhasker, Guillermo S. Christensen, Whitney E. McCollum, Jake Bernstein, Michael Culhane Harper

The US Supreme Court's (the Court) recent decision in *Chatrie v. United States*[1] marks another significant development in the Court's Fourth Amendment jurisprudence governing data privacy. Building on its decision in *Carpenter v. United States*[2] (which recognized Fourth Amendment protection for historical cell site location information), the Court held, by a 6–3 vote, that law enforcement's acquisition of Google's "Location History" data constitutes a Fourth Amendment search. The Court's reasoning reinforces the principle that individuals maintain a reasonable expectation of privacy in comprehensive digital location information even when that information is shared with and held by a third-party technology provider. Although this case arose from a criminal matter—a credit union robbery—its implications extend well beyond law enforcement investigations and into everyday life. Although the Fourth Amendment applies to government action rather than ordinary commercial data practices, the Court's reasoning may shape how regulators, courts, and litigants assess the sensitivity of location data and the adequacy of corporate governance controls. The Court's opinion reflects an increasingly sophisticated understanding of today's data-driven economy and underscores the legal significance of location data, behavioral data, and other sensitive personal information that companies routinely collect, retain, and disclose. The decision also has important implications for organizations that collect, retain, or disclose location information, particularly as courts, regulators, and legislatures continue to scrutinize commercial data governance practices.

BACKGROUND: GEOFENCES AND DATA COLLECTION

The case arose from a 2019 armed robbery investigation where law enforcement obtained a "geofence warrant" directing Google to identify devices that were present within a defined geographic area during a specified period (creating a "digital geographic fence" around the purported crime scene). The warrant initially required Google to search its vast repository of Location History data and produce anonymized records for devices within the designated area before investigators sought identifying information for specific accounts. That process ultimately led investigators to identify and charge their suspect, Chatrie.

The Court held that obtaining this Location History information constituted a Fourth Amendment search. Referencing its 2018 decision in *Carpenter*, the Court reasoned that Google's Location History creates a detailed record of an individual's movements and associations, revealing intimate aspects of daily life. The Court also rejected the government's argument that users forfeit constitutional protections simply because Google stores the information (third-party doctrine).

©2005-2026 K&L Gates LLP. All Rights Reserved.

The Court did not, however, determine whether the warrant itself satisfied the Fourth Amendment's probable cause requirements. It remanded the case to the lower courts for further proceedings.

WHY THIS MATTERS

Although *Chatrie* addresses constitutional limits on the government's access to data, the decision is likely to influence broader privacy rules and regulatory expectations.

First, the Court continued a trend of recognizing that digital data differs fundamentally from traditional business records. Rather than treating location information as transactional data voluntarily shared with a service provider, the Court emphasized the comprehensive and revealing nature of continuous digital location records—including where a person is at or near the time the data is generated. This reasoning may influence future disputes involving other forms of granular digital information, including precise GPS data, connected device data, and potentially artificial intelligence-derived behavioral profiles.

Second, the Court's analysis further narrows the traditional “third-party doctrine” in circumstances involving pervasive digital technologies. Companies should expect litigants, regulators, and courts to continue questioning whether individuals meaningfully consent to extensive data collection simply because they use modern digital services (as explained by the Court, users are continually prompted to opt in to location services in order to optimize an application's use).

Third, the opinion reinforces the growing recognition that location information occupies a special place within privacy law because it can reveal sensitive information about an individual's health, religion, political activities, employment, personal relationships, and daily routines. This principle increasingly appears across federal and state privacy statutes, Federal Trade Commission (FTC) enforcement actions, and international privacy frameworks. *Chatrie*'s characterization of location data as uniquely revealing may provide additional support for FTC enforcement and state attorney general actions targeting inadequate location data practices. State comprehensive and health-based privacy laws, including those in California, Texas, Virginia, Colorado, Washington, and Connecticut, classify precise geolocation as “sensitive data,” triggering opt-in consent requirements and heightened scrutiny.

Finally, although arising in a different legal context, *Chatrie* is consistent with a broader regulatory trend recognizing that precise geolocation information presents not only privacy concerns but also national security risks. Recent initiatives—including Executive Order 14117,[3] governing bulk transfers of sensitive personal data to countries of concern, and the Bureau of Industry and Security's Connected Vehicles Rule[4]—reflect an increasingly unified view across regulatory and national security frameworks that comprehensive location data warrants heightened legal protection.

PRACTICAL IMPLICATIONS FOR BUSINESSES

For organizations that collect or process location information, *Chatrie* serves as another reminder that sensitive data governance has become a strategic legal issue rather than merely a compliance exercise.

Companies should consider the following:

©2005-2026 K&L Gates LLP. All Rights Reserved.

- Reviewing what categories of location and mobility data are collected, how precise that data is, and whether all collection remains necessary for identified business purposes, including whether privacy-enhancing technologies, aggregation, de-identification, or less precise alternatives could satisfy the same business need.
- Reassessing retention periods for historical location information and other highly sensitive datasets.
- Evaluating internal governance surrounding responses to law enforcement requests, subpoenas, warrants, and other legal process involving customer data.
- Confirming that consumer-facing disclosures accurately describe location data collection, retention, sharing, and deletion practices.
- Monitoring how courts interpret *Chatrie* in future litigation involving geofence warrants and other forms of digital investigative techniques.
- Determining whether Executive Order 14117, the US Department of Justice's Data Security Program, or the Bureau of Industry and Security's Connected Vehicles Rule affect the organization's collection, transfer, or retention of sensitive location or other covered personal data.

LOOKING AHEAD

As data privacy continues evolving, *Chatrie* is unlikely to be the Court's last word on digital footprints. Because the Court expressly declined to determine the ultimate constitutionality of the geofence warrant at issue, significant questions remain regarding what degree of geographic scope, temporal scope, and particularity will satisfy the Fourth Amendment. Future cases will likely address those issues directly.

Beyond criminal investigations, however, the broader message is clear. Courts increasingly recognize that comprehensive digital datasets—particularly precise geolocation information—may warrant heightened legal scrutiny because of the insights they reveal about an individual's life. As legislatures, regulators, and courts continue to reshape privacy laws, organizations that collect sensitive personal information should anticipate greater expectations regarding transparency, necessity, data minimization, and governance.

FOOTNOTES

[1] 609 U.S. ___ (2026).

[2] 585 U.S. 296 (2018).

[3] 89 Fed. Reg. 15,421 (Feb. 28, 2024).

[4] 15 C.F.R. pt. 791, subpt. D (effective Mar. 17, 2025).

©2005-2026 K&L Gates LLP. All Rights Reserved.

KEY CONTACTS



SANJEEV BHASKER
PARTNER

WASHINGTON, DC, MIAMI, CHARLOTTE
+1.202.778.9260
SANJEEV.BHASKER@KLGATES.COM



WHITNEY E. MCCOLLUM
PARTNER

SEATTLE, SAN FRANCISCO
+1.206.370.7595
WHITNEY.MCCOLLUM@KLGATES.COM



MICHAEL CULHANE HARPER
PARTNER

WASHINGTON, DC
+1.202.778.4572
MICHAEL.HARPER@KLGATES.COM



GUILLERMO S. CHRISTENSEN
PARTNER

WASHINGTON, DC
+1.202.778.9095
GUILLERMO.CHRISTENSEN@KLGATES.COM



JAKE BERNSTEIN
GLOBAL AI AND INNOVATION PARTNER

SEATTLE
+1.206.370.7608
JAKE.BERNSTEIN@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.