

Location Technology and the U.S. Fourth Amendment

AUTHORS

Sipho C. Langa

AFFILIATIONS

UMD Tech Policy Hub
Phronesis Institute

How does the Fourth Amendment reasoning of Chatrie translate across the different technical ways that modern cellphone services generate or reveal a user's location data?



01. Introduction

In *Chatrie v. United States*, the U.S. Supreme Court held that police crossed a constitutional line when they obtained Google Location History data through a geofence warrant. The decision recognized that even limited cellphone location data can reveal private information about a person's movements, triggering Fourth Amendment protection. But the ruling leaves open how that reasoning applies to other cellphone services that generate or reveal location data. This project examines that gap across ride-sharing apps, social media platforms, and large language model chats.

02. Objective

This project aims to compare location-revealing mobile services to assess when law enforcement access to their data may trigger Fourth Amendment protection after *Chatrie*.

Related literature

THE FOURTH AMENDMENT AFTER *CHATRIE*

Digital Forensics for Mobility as A Service Platform: Analysis of Uber Application on iPhone and Cloud

Forensic analysis and privacy implications of LLM mobile apps: A case study of ChatGPT, Copilot, and Gemini

That's What Friends Are For: Inferring Location in Online Social Media Platforms Based on Social Relationships

03. Methodology

- ♦ **Coded** the *Chatrie* majority, concurrences, and dissents. Identify the technologies, data types, and legal principles addressed.
- ♦ **Reviewed** technical literature on how mobile services generate, store, and reveal location.
- ♦ **Classified** location data by source, precision, retention, and user involvement.
- ♦ **Assessed** whether each data type is explicitly covered, logically covered, excluded, or unresolved under each opinion.

04. Preliminary Findings

Chatrie most clearly protects precise cellphone location records held by a third party.

I

Coverage depends on how location is produced, not simply which service possesses it.

II

Protection becomes less certain when location is deliberately shared, coarsely derived, or inferred from other data.

III

The majority, concurrences, and dissents offer different rationales that may produce different outcomes for the same data.

IV



05. Analysis

I compare each service to Google Location History by asking how it creates or reveals location, how precise and persistent that data is, and whether police access would expose private patterns of movement.

Service Type	Location Data	Logical Coverage Under Chatrie	Supporting Language from Majority Opinion
Ride-sharing apps	GPS pickup/drop-off, routes, timestamps	Likely covered when precise location is automatically retained; disputed when knowingly provided to complete a trip	"any location-tracking service, whether Google's or some other company's."
Social Media Platforms	Check-ins, tags, photos, IP, inferred location	Mixed. Private, automatically generated GPS data are likely covered. Public geotags and deliberately shared locations are likely not. IP-derived location remains unresolved.	"just by doing the ordinary things cellphone users do."
Streaming Platforms	IP address, device data, regional access, listening/viewing patterns	Possibly covered when the service records direct device location. Coarse IP location and behavioral inferences remain unresolved.	The holding covers "historical cell phone location information," including information held by a third-party company.
LLM Chats	User text, uploads, metadata, IP/device signals	Unresolved. Direct device-location records may be covered; location voluntarily written in a prompt is less likely covered; inferred location presents the weakest analogy.	Information stored by a provider may remain private when "a user reasonably understands [it] as his own."

06. Next Steps and Feedback

This ongoing project will expand the comparison across mobile services, refine the framework for classifying location data, and examine how differences in precision, collection, disclosure, retention, and inference affect Fourth Amendment protection.

