

THE GOVERNMENT KNOWS WHAT YOU DID LAST SUMMER: HOW *CHATRIE V. UNITED STATES* REDEFINED THE FOURTH AMENDMENT FOR THE GEOFENCE ERA

*Taurus Myhand**

I. INTRODUCTION

Chatrie v. United States resolves a question the Supreme Court left open in *Carpenter v. United States*: whether law enforcement conducts a Fourth Amendment “search” when it compels a technology company to disclose location data drawn from millions of users rather than a single carrier’s records. The Court answers yes, holding that Google Location History is more revealing than cell-site data, that duration does not determine constitutional protection, and that the third-party doctrine does not reach data users experience as their own. Yet the decision resolves less than it appears to. By remanding the particularity question to the Fourth Circuit, the Court leaves geofence warrants—and the broader family of “reverse warrants” they inspired, including keyword searches, AI data demands, and mass video surveillance—without a governing standard for how narrowly such warrants must be drawn. Existing scholarship, including doctrinal mapping offered by amici in the case itself, treats this as a warrant-drafting problem to be solved through incremental particularity rules. This essay traces the case from the 2019 bank robbery through the Supreme Court’s decision, situates the ruling within the *Carpenter* line of precedent, and considers its implications for the broader universe of “reverse-search warrants,” including keyword searches, AI data requests, and video surveillance demands. It closes by previewing the

* Associate Professor of Law, Touro University, Jacob D. Fuchsberg Law Center; Ph.D., Criminology, Troy University, anticipated 2028; J.D., The University of Alabama School of Law, 2019; M.S.C.J., Troy University, 2011; B.S., Excelsior University, 2006. Former Corporate Litigation Associate at Richards, Layton & Finger, P.A., Wilmington, Delaware.

author's forthcoming dissertation, which argues that geofence and reverse-search technologies function as mechanisms of population-level social control rather than mere investigative tools.

Keywords: Fourth Amendment, geofence warrants, reverse warrants, digital privacy, third-party doctrine, mass surveillance, particularity requirement.

II. THE GOVERNMENT KNOWS WHAT YOU DID LAST SUMMER: HOW *CHATRIE V. UNITED STATES* REDEFINED THE FOURTH AMENDMENT FOR THE GEOFENCE ERA

The Supreme Court has issued its long-awaited decision in *Chatrie v. United States*, resolving one of the most consequential Fourth Amendment questions of the digital age: whether the government conducts a constitutional "search" when it uses a geofence warrant to obtain location data that Google collects from hundreds of millions of users. The Court's answer was yes, 6-3, and the implications extend far beyond Okello Chatrie's bank robbery conviction.

The case attracted enormous attention from the technology industry, legal scholars, civil liberties organizations, and law enforcement because the Court's answer will shape not only how police investigate crimes, but how broadly the government may use modern technology to identify and surveil ordinary Americans going about their daily lives.

III. HOW WE GOT HERE

In May 2019, Okello Chatrie walked into the Call Federal Credit Union in Midlothian, Virginia, armed with a handgun.¹ He threatened bank employees, forced customers to the ground, and escaped with \$195,000.² Because he was not apprehended at the scene, investigators were left without traditional leads. They turned instead to a relatively new investigative tool: a geofence warrant.³

A geofence warrant compels a technology company—in this case, Google—to search its databases for the identities of every device

¹ *Chatrie v. United States*, 146 S. Ct. 2193, 2202 (2026).

² *Id.*

³ *Id.*

that appeared within a defined geographic area during a defined time window. The warrant here targeted a 150-meter radius around the bank for one hour around the time of the robbery.⁴ Google responded through a three-step process it had developed to limit law enforcement's exposure to user data. At step one, it returned anonymized location data for nineteen accounts. At step two, without any new warrant, the investigating detective requested expanded location data covering a two-hour window for nine of those accounts. Google produced 680 data points. At step three, the detective requested identifying subscriber information for three accounts. One of them belonged to Chatrie.⁵ He was subsequently arrested, pleaded guilty conditionally, and was sentenced to 141 months in prison.

The district court found the warrant likely deficient for lack of particularized probable cause, but declined to suppress the evidence under the good-faith exception to the exclusionary rule.⁶ The Fourth Circuit, sitting en banc, upheld that result.⁷ The judges fractured badly on the underlying constitutional questions, producing multiple separate opinions without a clear majority rationale. The Supreme Court granted certiorari limited to a single question: whether executing the geofence warrant constituted a Fourth Amendment search.

IV. THE LEGAL LANDSCAPE BEFORE THE DECISION

The case arrived at the Court at the intersection of two lines of precedent that do not fit together easily.

The first is *Carpenter v. United States* (2018), in which the Court held that the government conducts a Fourth Amendment "search" when it obtains at least seven days of cell-site location information (CSLI) from a wireless carrier.⁸ Chief Justice Roberts wrote for the majority that the third-party doctrine—the principle that information voluntarily shared with a third party loses Fourth Amendment protection—does not apply when the data at issue is a

⁴ *Id.*

⁵ *Id.* at 2202-03.

⁶ *United States v. Chatrie*, 590 F. Supp. 3d 901, 905, 937-38 (E.D. Va. 2022), *aff'd*, 107 F.4th 319 (4th Cir. 2024), *vacated and remanded*, 146 S. Ct. 2193 (2026).

⁷ *United States v. Chatrie*, 107 F.4th 319, 325 (4th Cir. 2024), *vacated and remanded*, 146 S. Ct. 2193 (2026).

⁸ See *Carpenter v. United States*, 585 U.S. 296 (2018).

comprehensive chronicle of a person's physical movements.⁹ The Court emphasized both the revealing nature of location data and the fact that users do not meaningfully consent to its collection, since a cell phone logs its location automatically simply by being powered on.¹⁰

The second line concerns the warrant requirement itself: the Fourth Amendment's text demands that warrants "particularly describ[e] the place to be searched, and the persons or things to be seized."¹¹ A warrant that names no particular suspect but instead demands data on every person in a given area strains that requirement at its core.

The Fourth Amendment tension was plain. Chatrie argued that geofence warrants are constitutionally intolerable general warrants—the precise evil the Founders wrote the Fourth Amendment to prohibit. The government argued that the third-party doctrine governs, that two hours of location data is qualitatively different from the lengthy surveillance condemned in *Carpenter*, and that any constitutional defects are in any event cured by the good-faith exception.

V. WHAT THE AMICI SAID

Stanford Law School Professor Orin Kerr, whose academic work on the Fourth Amendment and digital technology has influenced this area for decades, filed as amicus offering a careful mapping of the issues. Professor Kerr argued that a properly drawn geofence warrant can satisfy the Fourth Amendment; that the Constitution does not present an all-or-nothing choice between zero protection and absolute protection. On the specific warrant at issue, Professor Kerr suggested step one was sufficiently narrow in time and space, but raised serious doubts about the constitutionality of steps two and three, which allowed officers to demand additional data without seeking a new warrant. His analysis of the warrant's three-stage structure foreshadowed the very questions the majority ultimately flagged for the Fourth Circuit on remand.

A coalition of technology scholars and civil liberties organizations filed in support of Chatrie, sounding an alarm about the broader implications for what they called "reverse warrants"—investigative techniques that start not with a known suspect but with a

⁹ *Id.* at 320.

¹⁰ *Id.*

¹¹ U.S. CONST. amend. IV.

mass of data from which police hope to identify one. The brief catalogued a rapidly expanding universe of such tools: reverse keyword search warrants that compel disclosure of every person who searched for a particular term; demands for data from AI chatbot providers; cloud searches; and video and image surveillance warrants. These tools, the brief argued, share a common constitutional defect—they sweep in data from thousands or millions of innocent people, capture overwhelmingly lawful and often highly sensitive behavior, and cast suspicion on individuals based on nothing more than their proximity, geographic or digital, to alleged criminal activity.

The United States argued for affirmance, contending that Chatrie voluntarily exposed his location data to Google and therefore forfeited any Fourth Amendment protection under the traditional third-party doctrine.¹² The government distinguished *Carpenter* on the grounds that two hours of location data—a brief, isolated window—bears no resemblance to the comprehensive surveillance condemned there.¹³ It further argued that even if the warrant was constitutionally deficient, the good-faith exception properly bars suppression, because at the time the warrant was issued no court had yet ruled geofence warrants unconstitutional and the detective acted in reasonable reliance on judicial authorization.

VI. THE COURT'S DECISION

Justice Kagan wrote for a majority that included Chief Justice Roberts and Justices Sotomayor, Kavanaugh, and Jackson. The vote was 6-3 on the outcome, though the majority and concurring opinions reflect real doctrinal disagreement beneath that surface alignment.

A. The Core Holding

The Court held that law enforcement officers conducted a Fourth Amendment search when they obtained Chatrie's Location History from Google.¹⁴ An individual has a reasonable expectation of privacy in cell phone location data, and the police invade that expectation when they demand it, regardless of whether the time

¹² Chatrie v. United States, 146 S. Ct. 2193, 2212 (2026).

¹³ *Id.* at 2209.

¹⁴ *Id.* at 2215.

period is short, and regardless of whether the data passes through a third-party company.¹⁵

B. Location History Is More Revealing Than CSLI

The majority reasoned that if *Carpenter* required a warrant for cell-site location information, a warrant is also required for Location History, which is superior in every relevant dimension.¹⁶ CSLI placed a user “within a ‘sector ranging from one-eighth to four square miles’”;¹⁷ Location History pinpoints location within roughly twenty meters.¹⁸ CSLI logged Carpenter's position an average of 101 times a day; Location History records location every two minutes, for a daily average of 720 data points.¹⁹ And unlike CSLI, Location History can estimate a phone's elevation, revealing which floor of a building a person occupies.²⁰ The majority concluded that when *Carpenter* described CSLI as providing a “detailed and encyclopedic” portrait of a person's movements, it did not yet know how much more revealing the next generation of technology would be.²¹

C. Duration Does Not Determine Whether a Search Occurs

The government's primary argument was that two hours of location data is not enough to trigger Fourth Amendment protection, and that *Carpenter* implicitly carved out a safe harbor for short-duration requests.²² The majority rejected this squarely. The Court noted that “even short-term monitoring” of physical movements can expose a person's visits to a psychiatrist, an abortion clinic, a criminal defense lawyer, or a political rally—exactly the sorts of associations the Fourth Amendment exists to protect.²³ More fundamentally, the Court held that the Fourth Amendment does not operate on a duration threshold: where it applies, “it applies—regardless of the ‘quality or

¹⁵ *Id.* at 2199.

¹⁶ *Id.* at 2213.

¹⁷ *Id.* at 2208, (quoting *Carpenter v. United States*, 585 U.S. 296, 312 (2018)).

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ *Id.*

²¹ *Id.*

²² *Id.* at 2209.

²³ *Id.* at 2210, (citing *United States v. Jones*, 565 U.S. 400, 415 (2012)).

quantity of information” obtained.²⁴ The government's approach would also create an unworkable series of line-drawing problems, such as, at what point does a non-search become a search?

D. The Third-Party Doctrine Does Not Reach Location History

The government argued, as it had in *Carpenter*, that a user who enables Location History has voluntarily shared his movements with Google and therefore forfeited any privacy interest in them.²⁵ The Court rejected this argument for reasons that track and extend *Carpenter's* logic. Location History is not “truly shared” in any meaningful sense.²⁶ Unlike bank records, which a customer hands over in the course of an arms-length commercial transaction, Location History is data that users experience as their own—they consult it, edit it, and use it as a personal journal of their travels.²⁷ The mere fact that Google stores it on its servers does not change that character, any more than storing photographs in Google Photos strips a user of any reasonable expectation that those photographs are private.²⁸

The majority also dismissed the government's argument that enabling Location History is a “voluntary” choice in a way that generating CSLI is not.²⁹ Google repeatedly prompts users to turn on the service, often warning that devices will not “work correctly” without it, while not disclosing how frequently location data would be recorded, how precise it would be, or how it might be shared with law enforcement.³⁰ More broadly, the Court refused to accept an app-by-app, feature-by-feature approach to Fourth Amendment protection that would effectively strip ordinary smartphone use of any constitutional coverage. The point of carrying smartphones, the Court observed, is to use the apps and services on them.³¹ That use cannot be severed from the simple act of carrying a turned-on phone.

²⁴ *Id.*, (quoting *Kyllo v. United States* 533 U.S. 27, 37 (2001)).

²⁵ *Id.* at 2212.

²⁶ *Id.* at 2213.

²⁷ *Id.* at 2209.

²⁸ *Id.*

²⁹ *Id.* at 2213.

³⁰ *Id.*

³¹ *Id.* at 2214.

E. The Warrant's Validity Remains for the Fourth Circuit

The majority was careful to limit its holding to the search question.³² Because the Fourth Circuit had concluded no search occurred, it never reached whether the geofence warrant satisfied the Fourth Amendment's requirements of particularity and probable cause at each of its three steps. The Court remanded for that analysis.³³ Justice Jackson, joined by Justice Sotomayor, concurred separately to signal that at least two members of the majority believe the warrant was deficient at steps two and three, where officers received expanding data without returning to a magistrate, leaving to their own unsupervised discretion who would face further scrutiny.³⁴ The Court also left untouched, for now, the question whether the good-faith exception would still bar suppression even if the warrant is found unconstitutional on remand.

F. The Concurrence and Dissents

Justice Gorsuch concurred in the judgment but wrote separately to criticize the majority's reliance on the *Katz* reasonable-expectation-of-privacy framework.³⁵ He would have grounded the result in traditional property principles, reasoning that Location History constitutes Chatrie's personal property—an "effect" within the meaning of the Fourth Amendment—and that the government searched it when it compelled Google to produce it.³⁶ Justice Alito dissented, joined in part by Justices Thomas and Barrett, arguing that the majority's opinion is both advisory (because the good-faith exception will likely bar relief on remand) and doctrinally unmoored, extending *Carpenter* well beyond the limits *Carpenter* itself claimed to draw, one of the fears Justice Alito expressed when *Carpenter* was decided.³⁷ Justice Barrett dissented separately on the ground that Chatrie had voluntarily shared his location data with Google and

³² *Id.* at 2215.

³³ *Id.* at 2216.

³⁴ *Id.* at 2217-18 (Jackson & Sotomayor, JJ., concurring).

³⁵ *See id.* at 2218-20 (Gorsuch, J., concurring).

³⁶ *Id.* at 2200-22.

³⁷ *Id.* at 2222-34 (Alito, J., dissenting).

therefore lacked a reasonable expectation of privacy under controlling precedent.³⁸

VII. WHY THIS DECISION MATTERS BEYOND THIS CASE

The practical significance of the ruling is substantial, even accounting for the limited scope of what was actually decided.

A. Geofence Warrants Now Require Genuine Fourth Amendment Justification

Law enforcement agencies that have used geofence warrants without rigorous particularity and probable cause analysis at each stage will need to revisit their practices. The Court's endorsement of the multi-step process as a workable framework, while expressly leaving open whether this particular warrant satisfied each step, suggests that narrowly drawn warrants may survive constitutional challenge, but that the days of relatively unchecked geofence requests are over.

B. The Third-Party Doctrine Is Further Constrained

The majority's refusal to apply the third-party doctrine to Location History, grounded in the argument that ordinary smartphone use does not amount to voluntary disclosure of one's movements to the government, signals that the doctrine's reach continues to erode in the context of modern digital data. The questions Justice Alito raises in dissent—where exactly does the line between *Carpenter* and *Miller* now run?—are genuine, and they will generate litigation.³⁹

C. Reverse Warrants More Broadly Are in the Crosshairs

As the technology scholars' amicus brief documented, whatever rule the Court announces in the location-data context will be tested by analogy against reverse keyword warrants, video surveillance demands, AI data requests, and other investigative tools that already exist. The majority's language—treating comprehensive third-party location databases as constitutional "panopticon[s]" from which law

³⁸ *Id.* at 2234 (Barrett, J., dissenting).

³⁹ *Id.* at 2233 (Alito, J., dissenting).

enforcement cannot freely draw—will be quoted in challenges to those tools for years to come.⁴⁰

D. The Particularity Question is Unresolved

The most practically important issue in the case, whether a three-step geofence warrant that names no suspect and provides no criteria for narrowing can satisfy the Fourth Amendment's particularity requirement, remains undecided. That question will return, and Professor Kerr's amicus brief, with its granular analysis of what particularity requires at each stage of a multi-step warrant, offers the most detailed available roadmap for how courts should approach it.

VIII. THE DEEPER CONSTITUTIONAL STAKES

When the Fourth Amendment was drafted, the Founders had lived under general warrants. General warrants were broad authorizations that permitted British officers to rummage through colonists' homes and papers in an unrestrained search for evidence of disloyalty. The particularity requirement was the Founders' direct response: a warrant must specify what is to be searched and what is to be seized. A warrant that demands identifying information on every person within 150 meters of a location for a specified hour names no person, describes no item to be seized, and rests on no individualized probable cause as to anyone.

At the same time, courts and commentators have long recognized the tension between privacy and public safety. The facts of *Chatrle* illustrate that tension vividly. A violent armed robbery was committed. Police had no suspects. A geofence warrant confined to 150 meters and one hour ultimately helped identify the perpetrator and close the case. There is nothing inherently unreasonable about law enforcement using available technology to investigate serious crimes, and the Fourth Amendment's touchstone panopticon—reasonableness—is capacious enough to accommodate that reality.

What *Chatrle* holds is that the government cannot bypass the constitutional warrant process simply because it is asking for location data rather than papers, or because it is directing its demand at a technology company rather than entering a physical home. The Fourth

⁴⁰ *Id.* at 2210 (majority opinion).

Amendment means what it says: warrants must be grounded in probable cause and must describe with particularity what is to be searched and seized. Those requirements apply in the digital age just as they did when the Founders wrote them.

The Fourth Circuit now has the task of applying those requirements to a three-step warrant that at least some members of this Court appear ready to find deficient. The outcome on remand will matter greatly for Chatrle and for the future of geofence warrants as an investigative tool. But the broader principle the Court announced today—that Location History is protected, that duration does not determine whether a search occurs, and that ordinary smartphone use does not strip Americans of Fourth Amendment rights—is now settled law.

This author is examining these questions in greater depth in a forthcoming criminology dissertation exploring the constitutional inadequacy of Fourth Amendment doctrine as applied to geofence warrants and reverse-search technologies. The dissertation is grounded in surveillance theory and social control scholarship. The core theoretical argument is that geofence warrants and reverse-search technologies function not merely as investigative instruments but as mechanisms of population-level social control.