Geofence Warrants After *Chatrie*: A Proposal for a Model Warrant

by Charles Kim[*]

The Supreme Court's decision in Chatrie v. United States *fundamentally altered the constitutional landscape governing so-called "geofence warrants" by holding that when the government acquires comprehensive location history data, it must first obtain a warrant which satisfies the Fourth Amendment's probable cause and particularity requirements. But* Chatrie *left a critical question unanswered: how would a constitutionally valid geofence warrant meet those requirements? This Contribution argues that the warrant at issue in* Chatrie *fell short because it authorized an increasingly intrusive search while leaving nearly every consequential decision to law enforcement officers rather than a neutral magistrate. Although anonymization of location data can substantially mitigate the privacy concerns associated with its disclosure, it is meaningful only if accompanied by safeguards that prevent premature de-anonymization. Building on these principles, this Contribution proposes a model geofence warrant that would require renewed judicial authorization before each expansion of the search. By restoring judicial oversight, the model warrant better reconciles legitimate law enforcement needs with the Fourth Amendment's historical commitment to protecting privacy from unbounded government discretion.*

In recent years, so-called "geofence warrants" have emerged as a novel but increasingly common investigative tool for law enforcement seeking to solve crimes. Their growing use has generated substantial litigation and scholarly debate, culminating in the Supreme Court's recent decision in *Chatrie v. United States*.[1]

Geofence warrants are typically used when law enforcement cannot identify a suspect through traditional investigative

[*] Charles Kim is a J.D. Candidate (2027) at New York University School of Law. This Contribution is a commentary on the problem at the 2026 Herbert Wechsler National Criminal Moot Court Competition hosted by the University at Buffalo School of Law.

[1] Chatrie v. United States, 146 S. Ct. 2193 (2026).

methods.[2] Rather than beginning with a known individual, investigators start with a known location and time where a crime occurred.[3] They then compel a technology company to disclose location data for every device within a defined geographic area during the relevant time period.[4] Investigators work to narrow the pool of devices and identify a suspect based on the device-associated location data.[5]

In an era in which cell phones continuously generate detailed records of their users' movements, geofence warrants offer investigators a powerful means of solving otherwise unsolvable crimes. Indeed, geofence warrants have helped revive cold cases[6] and, in *Chatrie* itself, identify a bank robber after traditional investigative methods proved unsuccessful.[7] At the same time, they sweep in the location information of countless innocent individuals, raising profound concerns about privacy and the limits of government surveillance. Accordingly, the debate surrounding geofence warrants has largely centered on a threshold constitutional question: whether obtaining this location data is sufficiently intrusive of privacy to constitute a "search" within the meaning of the Fourth Amendment.[8] If obtaining location data is a search, law enforcement generally must obtain a warrant that satisfies the Fourth Amendment's probable cause and particularity requirements;[9] if it is not a search, no warrant is required.[10]

Before *Chatrie*, courts and judges divided sharply on that issue. The Fifth Circuit adopted a categorical prohibition on geofence warrants, whereas several judges on the Fourth Circuit suggested

---

[2] *See* Haley Amster & Brett Diehl, Note, *Against Geofences*, 74 STAN. L. REV. 385, 388 (2022).
[3] *Id.*
[4] *Id.* at 388–89.
[5] *Id.*
[6] *Id.* at 388.
[7] *Chatrie*, 146 S. Ct. at 2202–03.
[8] *See, e.g.*, Lily Van Petten, Contribution, *Search by Geofence Warrant: Why Location Sharing Does Not Relinquish Fourth Amendment Rights*, 2025 N.Y.U. PROCEEDINGS 1, 3.
[9] Riley v. California, 573 U.S. 373, 381–82 (2014).
[10] Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

that such warrants did not constitute a search at all.[11] Other courts avoided the more difficult constitutional questions at play by finding that, because law enforcement officers had relied on a good-faith belief in the warrants' constitutionality, prosecutors could still use the evidence obtained at trial.[12]

Chatrie fundamentally altered that landscape. For the first time, the Supreme Court held that geofence warrants which allow the government to obtain a user's "Location History" data invade that person's reasonable expectation of privacy and therefore constitute a Fourth Amendment search.[13] Yet the Court declined to resolve the equally important question of whether the warrant before it satisfied the Fourth Amendment's separate requirements of probable cause and particularity, remanding those issues to the Fourth Circuit for further proceedings.[14] Only Justices Jackson and Sotomayor would have concluded that the warrant itself was constitutionally deficient.[15]

That unresolved question is now the central challenge in geofence warrant litigation. If obtaining location data triggers the Fourth Amendment's probable cause and particularity requirements, what should a constitutionally valid geofence warrant look like? This Contribution argues that the warrant in *Chatrie* itself fell short, and it proposes a model geofence warrant that better accommodates both legitimate law enforcement needs and the privacy interests the Fourth Amendment protects.

To begin, consider the warrant at issue in *Chatrie* itself. There, investigators sought location data maintained by Google through its "Location History" feature, which allows Google to record

---

[11] United States v. Smith, 110 F.4th 817, 838 (5th Cir. 2024), *cert. denied*, 146 S. Ct. 356 (2025) ("[W]e hold that geofence warrants are general warrants categorically prohibited by the Fourth Amendment."); United States v. Chatrie, 136 F.4th 100, 109 (4th Cir. 2025) (en banc) (Wilkinson, J., concurring) ("[T]here was no search here."), *vacated*, 146 S. Ct. 2193 (2026).

[12] *See Chatrie*, 136 F.4th at 100 (per curiam) (affirming the denial of suppression); *see also id.* at 101 (Diaz, C.J., concurring) ("I join in affirming the district court's denial of Okello Chatrie's suppression motion, but solely on the court's finding of good faith.").

[13] *Chatrie*, 146 S. Ct. at 2199.

[14] *Id.* at 2216–17.

[15] *Id.* at 2217 (Jackson, J., concurring).

users' locations as they carry their mobile devices.[16] The resulting data is remarkably precise. As the Supreme Court observed, Location History can identify not only where a user travels, but even what floor the user is located on within a multi-story building.[17]

After Google first received a geofence warrant in 2016, it developed a three-step process for responding to such requests.[18] At Step One, law enforcement specifies a geographic area and time period corresponding to the crime under investigation.[19] Google then identifies every device with Location History data falling within those parameters and provides investigators with anonymized device identifiers, accompanied by each device's location coordinates, timestamps, confidence intervals, and the source of the location data, such as GPS or Wi-Fi.[20]

At Step Two, investigators review the anonymized results and may request additional location data for selected devices identified in the first disclosure.[21] Google then provides expanded—but still anonymized—information concerning those devices' movements both inside and outside the original geofence over a broader period of time.[22]

Finally, at Step Three, investigators request identifying subscriber information for the devices they believe are relevant to the investigation, including the account holders' names and email addresses.[23] The staged disclosure process is significant because it incrementally expands law enforcement's access to increasingly sensitive information. Investigators begin with anonymous location data, proceed to detailed movement histories, and ultimately obtain the identities of selected users.

---

[16] United States v. Chatrie, 590 F. Supp. 3d 901, 907–09 (E.D. Va. 2022), *aff'd*, 107 F.4th 319 (4th Cir. 2024), *aff'd per curiam*, 136 F.4th 100 (4th Cir. 2025), *vacated*, 146 S. Ct. 2193 (2026).
[17] *Chatrie*, 146 S. Ct. at 2208.
[18] *Chatrie*, 590 F. Supp. 3d at 914.
[19] *Id.* at 914–15.
[20] *Id.*
[21] *Id.* at 916.
[22] *Id.*
[23] *Id.*

Yet although the search unfolds in three distinct stages, judicial authorization does not necessarily do the same. The warrant in *Chatrie* authorized the entire process at the outset, leaving virtually every consequential narrowing decision to investigators and, at times, to Google itself.[24] That structure—not merely the breadth of the search—was the warrant's principal constitutional defect.

The Fourth Amendment requires all warrants to be sufficiently particularized and supported by probable cause.[25] Although distinct requirements, they operate in tandem. Probable cause means a "fair probability" that evidence of a crime will be found in the place to be searched,[26] evaluated under the totality of the circumstances at the time the warrant is issued.[27] It is a practical, common-sense standard that requires only a "reasonable ground for belief of guilt"[28] and not "a prima facie showing" of criminal activity,[29] but it nonetheless demands individualized justification.[30] As the Supreme Court emphasized in *Ybarra v. Illinois*, a person's mere proximity to suspected criminal activity, without more, does not establish probable cause to search that person.[31]

The particularity requirement serves a different but related purpose. Whereas probable cause requires sufficient justification to conduct a search in the first instance, particularity limits the scope of that search by cabining law enforcement's discretion over

---

[24] *See Chatrie*, 590 F. Supp. 3d at 918–22 (describing the warrant and the lack of magistrate oversight over the three-step process).
[25] U.S. CONST. amend. IV.
[26] Illinois v. Gates, 462 U.S. 213, 238 (1983).
[27] *Id.* at 230–31.
[28] Maryland v. Pringle, 540 U.S. 366, 371 (2003) (quoting Brinegar v. United States, 338 U.S. 160, 175 (1949)).
[29] *Gates*, 462 U.S. at 235 (quoting Spinelli v. United States, 393 U.S. 410, 419 (1969), *abrogated on other grounds by* Gates, 462 U.S. 213).
[30] *See* Ybarra v. Illinois, 444 U.S. 85, 91 (1979) (holding that probable cause to search a tavern and bartender did not support searches of every customer at the tavern).
[31] *Id.*

what may be searched and seized.[32] Accordingly, the Fourth Amendment requires warrants to meaningfully constrain executive discretion by limiting the search to "the specific areas and things for which there is probable cause to search."[33]

These requirements reflect the central historical evil against which the Fourth Amendment's Warrant Clause was directed: the British Crown's use of general warrants and writs of assistance.[34] General warrants authorized officers to search on little more than suspicion while placing virtually no limits on where they could search or what they could seize.[35] Writs of assistance were similarly expansive, empowering customs officials to enter homes and businesses in search of contraband[36] and compel the assistance of peace officers—and, if necessary, nearby citizens—in executing those searches.[37]

The Colonists regarded these instruments as among the most notorious abuses of British authority, repeatedly protesting their use in the years preceding the Revolution.[38] The Warrant Clause

---

[32] *See* Arizona v. Gant, 556 U.S. 332, 345 (2009) (footnote omitted) ("Indeed, the character of that threat implicates the central concern underlying the Fourth Amendment—the concern about giving police officers unbridled discretion to rummage at will among a person's private effects.").

[33] Maryland v. Garrison, 480 U.S. 79, 84 (1987).

[34] *See* Riley v. California, 573 U.S. 373, 403 (2014) ("[T]he Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.").

[35] *See* Leonard W. Levy, *Origins of the Fourth Amendment*, 114 POL. SCI. Q. 79, 82 (1999) ("Officers or their informants merely reported that an infraction of the law had occurred or that they had a suspicion, not that a particular person was suspected or that a particular place contained evidence of a crime; on the basis of such an assertion, a magistrate issued a warrant.").

[36] *See* Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1260 (2016) ("[T]he first Townshend Act included a provision that gave customs officers the authority 'to enter houses or warehouses, to search for and seize goods prohibited to be imported or exported . . . or for which any duties are payable, or ought to have been paid.'" (citation omitted)).

[37] *See* Levy, *supra* note 35, at 84 (noting that writs of assistance permitted a crown official to command "the assistance, if necessary, of all nearby subjects in his execution of the writ.").

[38] *See Riley*, 573 U.S. at 403 ("Opposition to such searches was in fact one of the driving forces behind the Revolution itself.").

was adopted to ensure that such open-ended searches would not occur in the new Republic.[39] Measured against this historical background, the warrant in *Chatrie* failed the requirements of probable cause and particularity.

At Step One, investigators obtained anonymized location data for every device within the geofence, regardless of whether there was any individualized basis to suspect its owner of criminal activity.[40] Properly enforced, anonymization substantially mitigates the privacy concerns associated with that initial disclosure because investigators receive only anonymous location points, not identifiable individuals.[41] The lack of individualized suspicion for each person caught in the geofence would then be appropriately balanced by the lesser degree of intrusion into privacy, accommodating the Fourth Amendment's protection of intimate activities and associations.[42]

However, anonymization is meaningful only if it is accompanied by safeguards that preserve the thin line between an anonymous data point and an identifiable person.[43] The warrant in *Chatrie* imposed few such safeguards. Instead, investigators could progressively narrow the pool of devices and, through

---

[39] *Id.*

[40] *Chatrie*, 590 F. Supp. 3d at 919–21.

[41] *See Chatrie*, 136 F.4th at 149 (en banc) (Berner, J., concurring) ("[A]nonymous Location History data is not particularly sensitive . . . .").

[42] *See* In re Search of Info. that is Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 90 (D.D.C. 2021) [hereinafter *Matter I*] ("[T]he two-step process can serve as a court-supervised filter, winnowing geofence results that are unlikely to provide useful evidence to the government, thereby further minimizing third-party privacy concerns.").

[43] *See* Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 343 (4th Cir. 2021) (en banc) ("Plaintiffs submitted research showing that, because people's movements are so unique and habitual, it is almost always possible to identify people by observing even just a few points of their location history."); *cf.* Brennan v. Dickson, 45 F.4th 48, 64 (D.C. Cir. 2022) (explaining that only the FAA—not law enforcement—may match a drone's nonpublic serial number to the owner's identity for only limited purposes related to airspace safety, thereby preventing law enforcement from linking otherwise anonymous location information to an identifiable individual absent further authorization).

increasingly granular location information, potentially infer their owners' identities without renewed judicial authorization.[44]

As Judge Berner observed in her concurrence to the Fourth Circuit's decision in *Chatrie*, anonymity is often illusory when paired with highly granular location histories.[45] A device that repeatedly appears overnight at a particular residence, for example, may be linked to its owner through publicly available property or address records, rendering formal de-anonymization largely unnecessary. Without meaningful judicial oversight prohibiting or policing such efforts, investigators could effectively identify individuals long before Step Three formally disclosed subscriber information. No sophisticated technology is required for that de-anonymization—only the ability to compare highly granular location histories with publicly available information.[46]

That transition from anonymous location data to identifiable individuals marks a far greater intrusion upon privacy than the initial disclosure itself.[47] In that respect, the warrant raised the same concern animating the Court in *Ybarra*: mere presence near criminal activity, not probable cause for each individual user, became the basis for increasingly intrusive government scrutiny.

The warrant likewise failed to satisfy the Fourth Amendment's particularity requirement because it left the search's expansion largely to the discretion of investigators rather than the issuing magistrate.[48] The Fourth Amendment assigns the responsibility

---

[44] *See Chatrie*, 136 F.4th at 149 (en banc) (Berner, J., concurring) (explaining that two hours of Google Location History data could reveal a user's path from home to office, permitting the government to "readily determine that individual user's identity by, for instance, looking at property records and running a LinkedIn search.").

[45] *See id.*

[46] *Id.*

[47] *See id.* at 150 ("Through its second request to Google, however, the Government obtained two hours of Location History data belonging to nine pseudonymized individuals. That Location History data was not confined to any geographic boundary. At the time of the second request, law enforcement could have predicted that the pseudonymized data would likely be traceable to Chatrie and the other Google users. As a result, it was non-anonymous.").

[48] *See Chatrie*, 146 S. Ct. at 2218 (Jackson, J., concurring) ("[T]he warrant left 'too much to the discretion of the officer[s] executing the order,' giving them a

of defining the scope of a search to a neutral and detached magistrate rather than the discretion of officers engaged in the investigation; otherwise, the central purpose of the Fourth Amendment—to prevent boundless, discretionary searches—would be frustrated.[49] But as the district court observed, "Google does not impose specific, objective restraints on the size of the geofence, the length of the relevant timeframe, or the number of users for which it will produce data."[50] If investigators sought an overly broad search, the principal check was not judicial review but *Google's* willingness to object and negotiate narrower parameters.[51] Even then, Google—not a neutral magistrate—effectively determined whether the request should be modified or whether compliance would be withheld.[52]

The same defect persisted throughout the remainder of the search. At Step Two, investigators could request expanded location histories extending well beyond the original geofence, yet the warrant imposed no meaningful geographic limitation on those additional disclosures and required no renewed judicial finding before the search expanded.[53] Instead, investigators were instructed only to make an effort or attempt to narrow the list of devices before requesting additional information.[54] Those vague directives did little to cabin executive discretion. Indeed, Google itself objected during the *Chatrie* investigation because the investigating detective sought to de-anonymize *every* Step One device.[55]

Viewed as a whole, the constitutional problem was not simply that the warrant authorized a broad search. Properly structured, geofence warrants may begin with a broad, albeit anonymous, collection of location data. The constitutional defect instead arose

---

'roving commission' to collect more data absent any justification to a magistrate." (quoting Berger v. New York, 388 U.S. 41, 59 (1967))).

[49] *See* Johnson v. United States, 333 U.S. 10, 13–14 (1948).

[50] *Chatrie*, 590 F. Supp. 3d at 915.

[51] *Id.*

[52] *Id.*

[53] *Id.* at 916 ("[A]t Step 2, no geographic barrier confines the information searched.").

[54] *Id.* at 919.

[55] *Id.* at 921.

because the warrant permitted that initially anonymous search to become an increasingly individualized one without requiring renewed judicial authorization. As the search became more revealing, the magistrate's role diminished, leaving nearly every consequential decision to investigators instead of the neutral judicial officer whom the Fourth Amendment places between the citizen and the police.

That defect, however, is not inherent to geofence warrants. Geofence warrants can serve an important role in solving crimes that might otherwise remain unsolved, but they may not do so by running roughshod over the Constitution. The solution to this problem is straightforward: preserve staged disclosure but require staged judicial authorization. Every meaningful expansion of the search should entail renewed approval from the issuing magistrate.

That process should begin before any data is produced. At Step One, the magistrate should require law enforcement to demonstrate that traditional investigative techniques have been exhausted or are unlikely to identify a suspect. Investigators should also be required to present the most precise reconstruction possible of the crime, including the relevant time window, the suspect's known movements before and after the offense, likely points of entry and exit, and any other relevant evidence, such as the possibility of accomplices.

Using that information, the magistrate—not Google or law enforcement—should establish temporal and geographic limitations that minimize the number of innocent devices captured by the initial search.[56] Where realistically feasible, the geofence should exclude nearby residences, apartment buildings, or other sensitive locations unlikely to contain evidence of the

[56] *See* In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345, 363 (N.D. Ill. 2020) ("Another example to satisfy particularity is exactly what the government did here: draw narrowly tailored geofence zones for a sufficiently limited amount of time (approximately 15-30 minutes), and minimize through that zone design and subsequent investigation the possibility of sweeping in large amounts of location data for uninvolved individuals.").

crime, reducing potential privacy intrusions.[57] The initial disclosure of data should also remain strictly and *truly* anonymized. Investigators should receive only anonymous device identifiers and the minimum amount of location information necessary to evaluate whether further investigation is warranted. And crucially, the warrant should *expressly* prohibit attempts to identify users through publicly available information or other means before judicial authorization is obtained. Anonymous devices should remain precisely that—anonymous—until the Fourth Amendment permits otherwise, ensuring that no person is subjected to a highly intrusive search before the government has obtained individualized justification for that intrusion.

At Step Two, the warrant should replace vague directives requiring investigators merely to attempt to narrow the list of devices.[58] Instead, investigators should be required to articulate objective reasons why each remaining device warrants further scrutiny.[59] Those reasons might include movement consistent with the suspect's known path, timestamps corresponding to the commission of the offense, or other location data suggesting involvement in the crime. If investigators seek expanded location histories outside the original geofence or timeframe, they should return to the magistrate and explain why that additional information is supported by probable cause. The decision to expand the search should belong to the court—not to investigators and certainly not to Google or a third-party technology company.

The same principle should govern Step Three. Before subscriber information is disclosed, investigators should again return to the magistrate and identify the specific devices they seek to de-anonymize together with the facts establishing probable cause as to each device.[60] To be sure, probable cause does not eliminate the possibility that innocent individuals may ultimately be

---

[57] *Id.*
[58] *Chatrie*, 590 F. Supp. 3d at 919.
[59] *See, e.g.*, *Matter I*, 579 F. Supp. 3d at 73–74 (requiring that law enforcement filter out devices that are likely not to be relevant to the investigation).
[60] *See id.* at 73–74 (requiring law enforcement to return to the court before de-anonymization of subscriber data).

searched.[61] The Fourth Amendment has never required certainty that a place being searched contains conclusive evidence of criminal activity.[62] But it does require that those decisions be made by a neutral magistrate rather than by investigators exercising "roving" authority and unbounded discretion.[63]

This revised process better satisfies both probable cause and particularity. Probable cause in the model warrant rests not on mere geographic proximity but on objective facts connecting particular devices to the crime, such as their movements, timing, or other corroborating evidence developed during the investigation. Particularity is likewise strengthened because each successive expansion of the search is authorized—and limited—by a magistrate instead of left to the discretion of law enforcement or a private technology company. The result is not a categorical prohibition on geofence warrants but a constitutional framework that preserves their investigative value while substantially reducing the privacy harms they impose on innocent individuals.

Critics will undoubtedly argue that requiring repeated judicial approval will slow investigations and burden law enforcement. It will. But that objection misunderstands the function of the Fourth Amendment. The Framers deliberately required judicial oversight because they distrusted unchecked executive discretion.[64] The inconvenience of returning to a magistrate is not a flaw in the constitutional design; it is one of its principal safeguards.[65] The Fourth Amendment requires conscious deliberation before the government intrudes upon private life. A model geofence warrant that restores meaningful judicial oversight at each stage of the search honors that constitutional command; the warrant in *Chatrie* did not.

---

[61] *See Pringle*, 540 U.S. at 371 (describing probable cause as a "reasonable ground for belief of guilt." (quoting *Brinegar*, 338 U.S. at 175)).
[62] *Id.*
[63] *Berger*, 388 U.S. at 59.
[64] *See Riley*, 573 U.S. at 403 ("Our cases have recognized that the Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.").
[65] Smith, 110 F.4th at 841 (Ho, J., concurring) ("[H]amstringing the government is the whole point of our Constitution.").