

THE *LEON* LOOPHOLE: HOW GOOD FAITH TURNED GEOFENCE WARRANTS INTO A DIGITAL DRAGNET

Deanna Dulske*

ABSTRACT

Across the United States, law enforcement has been using geofence warrants at a rapid rate. The use of geofence warrants compels technology companies like Google to reveal the location data for all users in a specific area and time. This Comment argues that such warrants violate the Fourth Amendment in a fundamental way. They infringe on reasonable expectations of privacy, replace proximity with individualized probable cause, and due to them granting officers unlimited discretion, lack particularity. Although courts recognize the constitutional flaws in these cases, they still invoke Leon's good-faith exception. This Comment argues that Leon should not be applied in this case since geofence warrants are devoid of any indication of probable cause and are so obviously deficient that no reasonable officer would rely on them.

However, because courts are hesitant to make any decision on the matter, this Comment sees that the best route to a solution is targeted legislation. Therefore, to restore meaningful Fourth Amendment protections, this Comment proposes the Geofence Location Data Access Act, which would sharply limit geofence use, mandate judicial oversight at every step, and prohibit searches of sensitive places. The Act would limit geofence use to serious crimes, cap data collection at twenty-five individuals, require step-by-step judicial oversight, and prohibit searches in sensitive locations like homes and places of worship.

* J.D. Candidate, Texas Tech University School of Law, 2027; Texas Tech Law Review, Volume 58, Staff Member; B.S. Political Science, B.S. Homeland Security, Mississippi College. The Author thanks Dean Jack Nowlin and Professor Geoffrey Corn for their valuable guidance and insightful direction throughout the writing process. The Author also thanks Michael Gross, J.D., for sparking the idea for this Comment, and her father, John Dulske, for his thoughtful advice and steadfast willingness to listen. Lastly, the Author thanks the Texas Tech Law Review Volume 58 staff members and editorial board for their dedicated efforts and unwavering support during every stage of this project.

TABLE OF CONTENTS

ABSTRACT	565
I. INTRODUCTION	568
II. CASTING THE NET: THE RISE OF GEOFENCE WARRANTS AND THEIR EXPANDING REACH	570
A. <i>Inside the Geofence: What These Warrants Are and How They Work</i>	570
B. <i>Google as Gatekeeper: The Three-Step Identification Process</i>	572
C. <i>Old Doctrine, New Surveillance: The Fourth Amendment in the Digital Age</i>	573
D. <i>Judicial Division and the Leon Problem</i>	574
III. A SEARCH WITHOUT LIMITS: WHY GEOFENCE WARRANTS VIOLATE THE FOURTH AMENDMENT	576
A. <i>You Shared Your Data, Not Your Rights: The Reasonable Expectation of Privacy in Geofence Warrants</i>	576
1. <i>Location History Data Creates a Comprehensive Record of Private Life</i>	577
2. <i>The Third-Party Doctrine Does Not Apply to Geofence Warrants</i>	578
B. <i>Suspicion by Proximity: The Collapse of Probable Cause in Geofence Warrants</i>	580
1. <i>Being Near the Scene Is Not Enough</i>	581
2. <i>The “Inverted Probable Cause” Problem</i>	583
3. <i>Systematic Overbreadth: Evidence from the Real World</i>	583
4. <i>The Multi-Step Structure Amplifies the Probable Cause Deficiency</i>	584
C. <i>A Warrant Without Particularity: When No One Knows Who or What Is Being Searched</i>	585
IV. THE GOOD-FAITH EXCEPTION SHOULD NOT APPLY TO GEOFENCE WARRANT SEARCHES	588
A. <i>Magistrate Approval of Geofence Warrants Reflects a Structural Breakdown of Judicial Oversight</i>	588
1. <i>Magistrate Judges Giving Judicial Power to a Private Corporation Is the Magistrate Judge Abandoning Their Role</i>	589
2. <i>Magistrate Judges Rubberstamping Geofence Warrants Is an Error and Leaves a Powerless Corporation in Charge</i>	591
3. <i>Although Not Dispositive, Magistrate Error Needs to Be Analyzed Nonetheless</i>	592
B. <i>Beyond the Four Corners: Geofence Warrants So Lacking in Probable Cause That No Reasonable Officer Could Rely on Them</i>	593

1. <i>The Rejection of Proximity-Based Suspicion Is Not New or Obscure</i>	593
2. <i>The Affidavits Supporting Geofence Warrants Are Filled with Boilerplate Language and Are Conclusory</i>	594
C. <i>When Particularity Becomes a Guessing Game: Warrants So Facially Deficient that Officers Cannot Presume Them Valid</i>	599
1. <i>Fourth Amendment Commands Are Unambiguous</i>	600
2. <i>Geofence Warrants Not Only Dodge Particularity, They Flip It Upside Down</i>	600
3. <i>Google's Three-Step Process Invites, Rather Than Controls, Discretion</i>	601
V. LEGISLATION IS THE ANSWER: THE GEOFENCE LOCATION DATA ACCESS ACT	604
VI. CONCLUSION	607
APPENDIX	609

I. INTRODUCTION

A morning cyclist rides past a burglarized home.¹ Days later, police arrive at his door, not because of witness statements or forensic evidence, but because his phone was in the wrong place at the wrong time.² This is not a hypothetical or an excerpt from a dystopian novel, this is the result of when novel technology goes unchecked.³ Welcome to the era of geofence warrants, where one of law enforcement's most potent and controversial surveillance tools has been used unchecked.

These “reverse location” warrants compel providers to locate—within a gargantuan database—all devices that were in a particular place and time.⁴ This is done without the slightest showing of suspicion for any individual device.⁵ What starts out as an attempt to find an unknown suspect turns into a digital dragnet capturing innocent bystanders, worshippers, patients, and residents, prioritizing investigative ease over Fourth Amendment protections.⁶

The United States Supreme Court decided in *Carpenter v. United States* that long-term access to historical cell-site location information (CSLI) is a search.⁷ Nonetheless, geofence warrants are more precise and can be used retrospectively.⁸ There is a sharp divide in judicial responses on their validity.⁹ And yet, virtually every court admits evidence obtained from a geofence warrant through *Leon*'s good-faith exception.¹⁰ Courts defer to magistrate approvals that routinely delegate probable cause and particularity

1. John Schuppe, *Google Tracked His Bike Past a Burglarized Home. That Made Him a Suspect*, NBC NEWS (Mar. 7, 2020, at 05:22 CST), <https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761> [<https://perma.cc/CT66-RZ2Q>].

2. *Id.*

3. *Id.*

4. NAT'L ASS'N OF CRIMINAL DEF. LAWYERS, GEOFENCE WARRANT PRIMER 1 (2022), <https://www.nacdl.org/getattachment/816437c7-8943-425c-9b3b-4faf7da24bba/nacdl-geofence-primer.pdf> [<https://perma.cc/JJQ5-QCBL>]; see also Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from a “Geofence” General Warrant at 3, *United States v. Chatrie*, 590 F. Supp. 3d 901 (E.D. Va. 2022) (No. 3:19-cr-00130-MHL), 2019 WL 8227162 [hereinafter Google Amicus Brief] (explaining that geofence warrants require providers to search location-history databases to identify all devices within a defined geographic area during a specified time).

5. See Google Amicus Brief, *supra* note 4, at 10.

6. *Id.*

7. *Carpenter v. United States*, 585 U.S. 296, 313 (2018).

8. See Google Amicus Brief, *supra* note 4, at 10.

9. *Compare* *United States v. Smith*, 110 F.4th 817, 826 (5th Cir. 2024) (holding geofence warrants categorically unconstitutional as general warrants), *with* *United States v. Chatrie*, 136 F.4th 100, 100 (4th Cir. 2025) (en banc) (per curiam) (issuing fractured opinion declining to resolve constitutional validity).

10. See, e.g., *Chatrie*, 136 F.4th at 101 (Diaz, C.J., concurring) (applying good-faith exception); *id.* at 114 (Niemeyer, J., concurring) (finding good-faith reliance on the warrant); *id.* at 115 (King, J., concurring) (concluding officers acted in good faith); *id.* at 115 n.1 (Wynn, J., concurring) (recognizing good-faith reliance by officers); *id.* at 142–43 (Heytens, J., concurring) (relying on good-faith exception); *Smith*, 110 F.4th at 840 (applying good faith despite finding constitutional violations).

determinations to law enforcement and private corporations.¹¹ This “*Leon* problem,” allows structural flaws such as overbroad initial collections, unchecked officer discretion in narrowing the data, and rubberstamped warrants to persist.¹²

This Comment argues that geofence warrants violate the Fourth Amendment’s core protections. They collect data subject to a reasonable expectation of privacy,¹³ lack probable cause by substituting proximity for individualized suspicion,¹⁴ and lack particularity by granting unlimited discretion like the historical colonial writs of assistance.¹⁵ Thus, the good-faith exception cannot keep rescuing evidence obtained from a geofence warrant because it falls under *Leon*’s exceptions.¹⁶ Judicial band-aids are not enough; Congress must enact targeted legislation.¹⁷ Just as it regulated wiretaps through Title III of the Omnibus Crime Control and Safe Streets Act, Congress must now step in to regulate geofence warrants.¹⁸ By proposing the Geofence Location Data Act, this Comment not only critiques these issues but also offers a practical legislative path forward.

This Comment proceeds in five Parts. Part II explains what geofence warrants are, how they operate through Google’s three-step process, and how courts have responded to them.¹⁹ Part III demonstrates why geofence warrants violate the Fourth Amendment by infringing reasonable expectations of privacy, lacking probable cause, and failing the particularity requirement.²⁰ Part IV argues that the good-faith exception does not apply because these warrants reflect magistrate abandonment of the judicial role,

11. *Smith*, 110 F.4th at 826 (analogizing geofence warrants to general warrants); *People v. Meza*, 312 Cal. Rptr. 3d 1, 18 (Cal. Ct. App. 2023) (applying good faith despite finding evidence “devoid of any detail . . . that would have supported a finding of probable cause”); *see also Chatrie*, 136 F.4th at 155 (Gregory, J. dissenting) (under warrant’s terms, “Google, not a magistrate, was the sole entity that could confine the scope of the ultimate search[]”).

12. *See also United States v. Chatrie*, 590 F. Supp. 3d 901, 918 (E.D. Va. 2022), *aff’d en banc*, 107 F.4th 319 (4th Cir. 2024), *aff’d on reh’g*, 136 F.4th 100 (4th Cir. 2025), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026) (demonstrating where a magistrate asked no questions and made no changes despite sweeping a 300-meter search area).

13. *See Carpenter v. United States*, 585 U.S. 296, 311 (2018) (recognizing cell phones follow owners into private spaces, revealing intimate details); *infra* Section III.A (explaining how geofence warrants invade a person’s reasonable expectation of privacy).

14. *See infra* Section III.B (showing how the government uses proximity as a substitute for individualized suspicion).

15. *See generally Smith*, 110 F.4th at 826–36 (discussing historical general warrants and writs of assistance).

16. *See infra* Part IV (arguing against the good-faith exception rescuing evidence simply by falling under *Leon*’s exceptions).

17. *United States v. Chatrie*, 136 F.4th 100, 112 (4th Cir. 2025) (Diaz, C.J., concurring) (“This type of compromise is a classic legislative task. Applying the exclusionary rule categorically to geofence warrants preempts legislative input in an area whose real impact upon the body politic would seem to invite some measure of popular participation.”).

18. *Id.*

19. *See infra* Part II (explaining how courts have responded to geofence warrants).

20. *See infra* Part III (exemplifying the Fourth Amendment violations geofence warrants cause).

contain affidavits so devoid of probable cause that no reasonable officer could rely on them, and are so facially deficient that officers cannot presume them valid.²¹ Finally, Part V proposes the Geofence Location Data Access Act: legislation modeled after Title III that would limit geofence use and give law enforcement a set guideline.²²

II. CASTING THE NET: THE RISE OF GEOFENCE WARRANTS AND THEIR EXPANDING REACH

To understand why geofence warrants violate the Fourth Amendment, one must first understand how they operate. This Part explains the technical and legal foundation needed to evaluate their constitutionality. Section A explains what geofence warrants are and how they are different from traditional warrants.²³ Section B lays out Google's three-step process that has become the national standard for executing these searches.²⁴ Section C places geofence warrants within the changing world of Fourth Amendment jurisprudence.²⁵ Finally, Section D looks at the judicial division over geofence warrants' validity and introduces the "*Leon* problem."²⁶ Together, these Sections explain not a novel investigation technique, but a complete departure from Fourth Amendment principles that threatens to normalize warrantless mass surveillance.

A. Inside the Geofence: What These Warrants Are and How They Work

Geofence warrants compel third-party companies to provide location data of users for all those who were in a certain area during a specific timeframe, aiming to identify unknown suspects.²⁷ Unlike traditional warrants, which target known suspects, geofence warrants work in reverse—without an initial suspect.²⁸

Most geofence warrants depend on the technology of Google's Location History data and Sensorvault database.²⁹ Location History data relies on GPS, Wi-Fi, and Bluetooth signals to automatically log a user's movement every

21. See *infra* Part IV (arguing against the good-faith exception).

22. See *infra* Part V (proposing model legislation).

23. See *infra* Section II.A (examining the differences between geofence warrants and traditional warrants).

24. See *infra* Section II.B (explaining Google's three-step process and the constitutional risks associated with it).

25. See *infra* Section II.C (examining the evolution of Fourth Amendment protections in the digital age).

26. See *infra* Section II.D (detailing a circuit split on the applicability of the good-faith exception to geofence warrants).

27. See Google Amicus Brief, *supra* note 4, at 3.

28. See *id.*

29. See *id.*

two minutes.³⁰ This results in tracking that is far more accurate than CSLI and can place a device within a few meters—sometimes even pinpointing the specific floor a device is on.³¹ Once enabled, Google tracks location data continuously—even when users are not actively using their devices.³²

Google has made the activation easy through its interface, which essentially prompts users across all apps to enable the feature when opening them.³³ However, this story is quite different for a user who opts-in and later decides to opt-out because the disabling option is hidden behind complex settings menus.³⁴ By 2018, Google was tracking over 592 million people worldwide.³⁵ This data is not safe from law enforcement, as Google reported that law enforcement requests for this data have grown exponentially, and the Sensorvault has become a primary target for geofence search warrants.³⁶ This issue spans across the technology world: Google, Apple, and Meta jointly disclosed location data from 3.16 million users in response to geofence warrants and similar requests.³⁷

These warrants have been used across a wide range of investigations from bank robberies and post office burglaries,³⁸ to the January 6, 2021, Capitol events.³⁹ But these warrants produce “false positives,” sweeping up morning cyclists⁴⁰ and people still logged into old accounts.⁴¹

30. *See id.* at 4.

31. *See* Petition for Writ of Certiorari at 7, *Chatrle v. United States*, No. 25-112 (U.S. July 28, 2025) [hereinafter *Chatrle Pet. for Cert.*]; *see also* *United States v. Chatrle*, 590 F. Supp. 3d 901, 908–09 (E.D. Va. 2022), *aff’d en banc*, 107 F.4th 319 (4th Cir. 2024), *aff’d on reh’g*, 136 F.4th 100 (4th Cir. 2025), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026) (explaining how location history can estimate a device’s location with high precision).

32. *See* *Chatrle Pet. for Cert.*, *supra* note 31, at 7.

33. *See* *United States v. Smith*, 110 F.4th 817, 823 (5th Cir. 2024); *see also* Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), <https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html> [https://perma.cc/N2AW-TAK5] (explaining how police use of Google’s location data can harm innocent bystanders).

34. *Smith*, 110 F.4th at 835–36.

35. *Chatrle*, 590 F. Supp. 3d at 909.

36. *Global Requests for User Information*, GOOGLE, <https://transparencyreport.google.com/user-data/overview> [https://perma.cc/2VYS-J5BV] (last visited Feb. 24, 2026); *see also* Google Amicus Brief, *supra* note 4, at 3 (“Year over year, Google has observed over a 1,500% increase in the number of geofence requests it received in 2018 compared to 2017; and to date, the rate has increased over 500% from 2018 to 2019.”).

37. Kaaviya, *Google, Meta and Apple Fuel the World’s Largest Surveillance Machine*, CYBER SEC. NEWS (Mar. 4, 2025), <https://cybersecuritynews.com/google-meta-apple-fuel-surveillance/> [https://perma.cc/X27Z-2Z4Y].

38. *See generally* *Chatrle*, 590 F. Supp. 3d at 908–09 (bank robbery); *Smith*, 110 F.4th at 822–23 (post office burglary).

39. *United States v. Rhine*, 652 F. Supp. 3d 38, 44–46 (D.D.C. 2023) (describing geofence warrants in the January 6th Capitol investigation).

40. Schuppe, *supra* note 1.

41. Meg O’Connor, *Avondale Man Sues After Google Data Leads to Wrongful Arrest for Murder*, PHX. NEW TIMES (Jan. 16, 2020), <https://www.phoenixnewtimes.com/news/google-geofence-location-data-avondale-wrongful-arrest-molina-gaeta-11426374/> [https://perma.cc/3UZ9-6RJB].

B. Google as Gatekeeper: The Three-Step Identification Process

Geofence searches follow a three-step process, which is not a result of decisions made by Congress or courts, but rather Google and the Department of Justice's Computer Crime Section.⁴² In fact, this privately crafted procedure is the current framework in which geofence searches are conducted nationwide.⁴³

Step One begins with law enforcement obtaining a court order compelling Google to search the Sensorvault for all devices matching the warrant's location and time frame.⁴⁴ In response, Google provides a list that is anonymized and does not contain names or subscriber information.⁴⁵

Step Two, law enforcement has complete freedom to request more data from selected devices, often extending beyond the warrant's original boundaries.⁴⁶ This is not the only boundless element present in geofence warrants, as officers review the list provided by Step One, and apply their own judgment on which devices are "relevant."⁴⁷ After the officer shortens the list, they will ask Google to provide more detailed location tracking for the selected devices.⁴⁸ However, there is no objective standard for this selection process, and no additional court approval is required.⁴⁹

Step Three: Google discloses the real identities of the people whose devices were selected.⁵⁰ Here, officers will get the names, email addresses, and subscriber information attached to the device, thus transforming the previously anonymous data into searchable individuals.⁵¹ Just like in Step Two, this unmasking is generally done without renewed judicial review.⁵²

This structure creates profound constitutional problems because Steps Two and Three are frequently carried out without further judicial review—

42. See GEOFENCE WARRANT PRIMER, *supra* note 4, at 1–2.

43. See *infra* notes 45–52 (describing the three-step process as analyzed across jurisdictions).

44. See GEOFENCE WARRANT PRIMER, *supra* note 4, at 1–2.

45. *Id.*

46. *Id.*; see *United States v. Chatrie*, 590 F. Supp. 3d 901, 916 (E.D. Va. 2022), *aff'd en banc*, 107 F.4th 319 (4th Cir. 2024), *aff'd on reh'g*, 136 F.4th 100 (4th Cir. 2025), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026).

47. *United States v. Smith*, 110 F.4th 817, 825 (5th Cir. 2024) ("[L]aw enforcement reviews the anonymized list provided by Google and determines which IDs are relevant."); *People v. Meza*, 312 Cal. Rptr. 3d 1, 18 (Cal. Ct. App. 2023) (observing officers initially drew shapes because they "felt" those shapes might shrink the device pool, rather than because geometry corresponded to the crime scene).

48. *Smith*, 110 F.4th at 825.

49. *Meza*, 312 Cal. Rptr. 3d at 16 (observing geofence warrants provide no meaningful restriction on law enforcement discretion); *In re Search of Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 754 (N.D. Ill. 2020) (denying geofence warrant application because warrant imposed no limit on government's discretion to select device IDs for identifying subscriber information) [hereinafter *Pharma II*].

50. See GEOFENCE WARRANT PRIMER, *supra* note 4, at 4.

51. See GEOFENCE WARRANT PRIMER, *supra* note 4, at 4.

52. See *Meza*, 312 Cal. Rptr. 3d at 16.

delegating core probable cause determinations to Google and investigators⁵³ The initial warrant authorizes a broad sweep, but the crucial decisions about whose privacy to invade more deeply, and whose identity to unmask, are made through a process that circumvents the judicial gatekeeping role that the Fourth Amendment demands.⁵⁴ Currently, this structure allows overcollection and involuntary intrusions into innocent bystanders' privacy.⁵⁵

C. Old Doctrine, New Surveillance: The Fourth Amendment in the Digital Age

The Fourth Amendment protects people from unreasonable government searches.⁵⁶ Two basic rules flow from that protection: the government usually needs a warrant supported by probable cause, and the warrant must describe with some precision what or who will be searched.⁵⁷ The Fourth Amendment requires that a neutral and detached judge decide whether these two requirements are met.⁵⁸

Determining whether government action is a search often begins with the *Katz* reasonable-expectation-of-privacy test: (1) whether the individual has “exhibited an actual (subjective) expectation of privacy,” and (2) whether that expectation is “one that society is prepared to recognize as ‘reasonable.’”⁵⁹ However, the third-party doctrine (TPD) states that no one has a reasonable expectation of privacy regarding things voluntarily disclosed to third parties.⁶⁰ For much of the twentieth century, the TPD filled an essential role in enabling warrantless searches of information conveyed to third parties.⁶¹ Under the TPD, law enforcement is allowed to conduct a warrantless search of bank records, dialed telephone numbers, and similar transactional records.⁶² Such searches are generally outside the Fourth

53. See *United States v. Chatrue*, 136 F.4th 100, 158 (4th Cir. 2025) (Gregory, J., dissenting) (Detective Hylton requested Google de-anonymize three numbers without additional judicial oversight); *In re Search of Info. Stored at Premises Controlled by Google*, 2022 WL 584326, at *9 (police wanted to unilaterally tell Google which cell phones to unmask to obtain the owner's personal information).

54. See *Chatrue*, 136 F.4th. at 159 (Gregory, J., dissenting) (warrant ceded authority and decision-making from independent judicial officer to private corporation).

55. See *id.*

56. U.S. CONST. amend. IV (“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . .”).

57. *Id.* (“[N]o Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”).

58. See *Dalia v. United States*, 441 U.S. 238, 255 (1979) (requiring a neutral and detached magistrate to issue warrants).

59. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

60. *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979); *United States v. Miller*, 425 U.S. 435, 443 (1976).

61. *Smith*, 442 U.S. at 743–44; *Miller*, 425 U.S. at 443.

62. See *Miller*, 425 U.S. at 443 (no Fourth Amendment protection for bank records obtained from bank); *Smith*, 442 U.S. at 743–44 (no expectation of privacy in dialed telephone numbers conveyed to telephone company).

Amendment's protection because the individual had assumed the risk that the third party could disclose the information to the government.⁶³

The Supreme Court narrowed the application of the TPD in the context of digital surveillance in *Carpenter v. United States*.⁶⁴ The Court held that the government's acquisition of seven days or more of CSLI constitutes a Fourth Amendment search, which generally requires a warrant.⁶⁵ The Court distinguished CSLI data because it provided an "exhaustive chronicle of location information" that reveals "an intimate window into a person's life," capable of exposing their "familial, political, professional, religious, and sexual associations."⁶⁶

D. Judicial Division and the Leon Problem

The fast development of technology combined with the increased use of geofence technology has resulted in diverging opinions across federal and state courts, which has left the constitutional status of geofence warrants unsettled.⁶⁷ Some appellate courts have held that geofence warrants categorically violate the Fourth Amendment, while others have rejected such a categorical ban.⁶⁸ Nevertheless, this divergence is not only limited to circuit courts; this divergence has split circuits themselves.⁶⁹ In *Chatrie*, the court's fractured per curiam opinion consisted of multiple opinions that disagreed on these threshold questions.⁷⁰

United States v. Leon states that a when a warrant is later found to be unconstitutional, the evidence that was obtained under that warrant should not be suppressed if the officers reasonably relied on the magistrate's authorization.⁷¹ *Leon* recognizes exceptions to this good-faith rule: (1) the affidavit contains knowingly or recklessly false statements; (2) the magistrate wholly abandoned the judicial role; (3) the affidavit is so lacking in indicia of probable cause that belief in its validity is unreasonable; or (4) the warrant

63. See *Miller*, 425 U.S. at 443; *Smith*, 442 U.S. at 743–44.

64. *Carpenter v. United States*, 585 U.S. 296, 316–17 (2018).

65. *Id.*

66. *Id.* at 313 (internal quotations omitted).

67. Compare *United States v. Smith*, 110 F.4th 817, 826 (5th Cir. 2024) (holding geofence warrants categorically unconstitutional), and *Wells v. State*, 714 S.W.3d 614, 626 (Tex. Crim. App. 2024) (rejecting Fifth Circuit view), with *United States v. Rhine*, 652 F. Supp. 3d 38, 66–67 (D.D.C. 2023) (finding geofence warrants constitutional).

68. *Smith*, 110 F.4th at 826 (holding geofence warrants categorically unconstitutional); *United States v. Chatrie*, 590 F. Supp. 3d 901, 937 (E.D. Va. 2022), *aff'd en banc*, 107 F.4th 319 (4th Cir. 2024), *aff'd on reh'g*, 136 F.4th 100 (4th Cir. 2025), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026) (finding constitutional violations but applying good-faith exception); *Rhine*, 652 F. Supp. 3d at 66–67 (upholding geofence warrants).

69. *Chatrie*, 136 F.4th at 100–01 (issuing a one-sentence per curiam opinion with eight separate concurring opinions and one dissenting opinion).

70. *Id.* at 115 (Wynn, J., concurring) (criticizing the court's failure to address threshold constitutional questions).

71. *United States v. Leon*, 468 U.S. 897, 922 (1984).

is so facially deficient in its description of the place to be searched or the things to be seized that officers cannot reasonably presume it valid.⁷² When confronted with geofence search warrant challenges, many courts have admitted evidence obtained from a geofence warrant under this good-faith exception to the Fourth Amendment's exclusionary rule.⁷³

The result is a fragmented body of law with no clear answer. The Fifth Circuit in *United States v. Smith* directly confronted the constitutional issue geofence warrants present, and they held that geofence warrants categorically violated the Fourth Amendment.⁷⁴ The *Smith* court explained that such warrants were similar to general warrants because they failed to describe the persons or things to be seized.⁷⁵ The Fifth Circuit pointed out that the Fourth Amendment does not permit the government to carry out a search first and come up with probable cause later.⁷⁶

However, the district court in *United States v. Chatrie* permitted the evidence collected by the geofence warrant at issue only after applying the good-faith exception.⁷⁷ In the en banc rehearing, some judges on the court acknowledged serious constitutional deficiencies in the warrant's design; however, many refused to consider the underlying constitutional issue.⁷⁸ Instead, they said the law enforcement officer executed the warrant in good faith.⁷⁹ The per curiam opinion effectively side-stepped the underlying constitutional issue and left the validity of geofence warrants unresolved.⁸⁰

The disagreement between the circuits, with one side flat out refusing to address the validity of a geofence warrant, and the other side finding a categorical ban, has resulted in nobody knowing the time, conditions, or circumstances under which one can use a geofence warrant or conduct a geofence search.⁸¹ This lack of direction highlights the need for federal legislation like the Geofence Location Data Access Act, which would provide a standard for geofence use nationwide.⁸²

72. *Id.* at 923.

73. *See, e.g., Smith*, 110 F.4th at 840 (applying the good-faith exception).

74. *Id.* at 826.

75. *Id.*

76. *Id.* at 837.

77. *United States v. Chatrie*, 590 F. Supp. 3d 901, 937 (E.D. Va. 2022), *aff'd en banc*, 107 F.4th 319 (4th Cir. 2024), *aff'd on reh'g*, 136 F.4th 100 (4th Cir. 2025), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026).

78. *Chatrie*, 136 F.4th at 115 (4th Cir. 2025) (Wynn, J., concurring) (“[T]his Court squanders a critical opportunity to clarify the Fourth Amendment’s application to emerging surveillance technologies. Instead, we take shelter in the judge-made doctrine of ‘good faith,’ leaving both courts and citizens to grope in the dark as to the limits of governmental power in the digital age.”).

79. *Id.* at 101 (Diaz, C.J., concurring) (refusing to extend analysis beyond finding good faith).

80. *Id.* at 115 (Wynn, J., concurring) (acknowledging the court’s failure to reach a decision has left the public ignorant on geofence limits).

81. *See* Orin S. Kerr, *The Fourth Circuit’s Geofencing Case Ends Not with a Bang but a Whimper*, REASON (May 2, 2025, at 21:13 CST), <https://reason.com/volokh/2025/05/02/the-fourth-circuits-geofencing-case-ends-not-with-a-bang-but-a-whimper/> [<https://perma.cc/6AUV-Y8PJ>].

82. *See infra* Part V (proposing the Geofence Location Data Access Act).

III. A SEARCH WITHOUT LIMITS: WHY GEOFENCE WARRANTS VIOLATE THE FOURTH AMENDMENT

This Part explains how geofence warrants are unconstitutional searches under the Fourth Amendment. Geofence warrants fail all requirements for valid searches.⁸³ Section A argues that individuals have a reasonable expectation of privacy in their location history even if the data is shared with Google, and that the third-party doctrine does not eliminate this protection.⁸⁴ Section B describes how geofence warrants do not have probable cause because they switch proximity for individualized suspicion.⁸⁵ Section C shows that these warrants fail the particularity requirement by allowing indiscriminate searches and granting officers unbridled discretion.⁸⁶ Each of these deficiencies alone render geofence warrants unconstitutional, and together, they lead to the conclusion that these warrants—if left without congressional guardrails—are incompatible with the Fourth Amendment.

A. You Shared Your Data, Not Your Rights: The Reasonable Expectation of Privacy in Geofence Warrants

Geofence warrants are Fourth Amendment searches because they invade a person's "reasonable expectation of privacy in the whole of their physical movements."⁸⁷ Under the two-part test established in *Katz v. United States*, this expectation exists when (1) an individual subjectively seeks to preserve something as private, and (2) society recognizes that expectation as objectively reasonable.⁸⁸ When a geofence warrant is used to compel Google to disclose Location History data for all devices within a defined area, it goes against both prongs of this test as it reveals extremely personal aspects of a person's life.⁸⁹

83. See *infra* Part III (explaining how geofence warrants fail to meet Fourth Amendment requirements).

84. See *infra* Section III.A (explaining privacy interests in data shared with third parties).

85. See *infra* Section III.B (explaining probable cause requirements of the Fourth Amendment in relation to search warrants).

86. See *infra* Section III.C (explaining how geofence warrants are akin to general warrants that the Fourth Amendment prohibits).

87. See *Carpenter v. United States*, 585 U.S. 296, 310 (2018) (citing *United States v. Jones*, 565 U.S. 400, 430 (2012) (Alito, J., concurring)).

88. *United States v. Katz*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

89. See *Carpenter*, 585 U.S. at 311 (location data "provides an intimate window into a person's life"); *United States v. Chatrie*, 136 F.4th 100, 105 n.5 (4th Cir. 2025) (en banc) (per curiam) (quoting *United States v. Chatrie*, 590 F. Supp. 3d 901, 907 n.5 (E.D. Va. 2022) ("Even Google—in an amicus brief—argued 'that a geofence is certainly a "search" within the meaning of the Fourth Amendment' because 'users have a reasonable expectation of privacy in the [Location History] information, which the government can use to retrospectively reconstruct a person's movements in granular detail.'").

I. Location History Data Creates a Comprehensive Record of Private Life

Location History data, by its nature, invokes a subjective expectation of privacy because it shows the most intimate sides of a person's life, such as where they sleep, where they go to church, where they get medical treatment, and where they attend political meetings.⁹⁰ Such a continuous and all-encompassing surveillance that reaches into constitutionally protected areas with a level of detail even greater than what CSLI can provide is absolutely protected by the Fourth Amendment.⁹¹

As demonstrated in Section II, Google continuously tracks users across all apps and devices linked to a Google account.⁹² This tracking achieves meter-level accuracy, and not only can it pinpoint a user's location but also the specific floor of the building they are in.⁹³ For example, in *Chatrie*, the 300-meter radius of the geofence encompassed not only the bank where the robbery took place, but also several private homes, a hotel, a church, and a senior living facility, thus recording the exact movements of worshippers, patients, residents, and passersby alike.⁹⁴

A geofence warrant, unlike a stakeout, which is limited to known suspects and physical barriers, allows the tracking of unknown individuals within private spaces.⁹⁵ Location History data and its ability to measure elevation, thereby identifying the specific floor in a building where a person might be, is analogous to the technology condemned in *Kyllo v. United States*.⁹⁶ The Court in *Kyllo* denounced thermal-imaging technology, which revealed details of a home's interior, holding that its use constituted a search.⁹⁷ Geofence searches collect Location History data and enable law enforcement to explore what was happening within the home or other private places.⁹⁸ Just as the technology in *Kyllo* allowed law enforcement to explore

90. See *Carpenter*, 585 U.S. at 311 (identifying categories of sensitive information revealed by location data).

91. See Google Amicus Brief, *supra* note 4, at 10 (explaining Location History data is capable of estimating location within twenty meters); see also *Chatrie*, 590 F. Supp. 3d at 908 (describing the breadth of details that cell phone warrants encompass).

92. See *Chatrie*, 590 F. Supp. 3d. at 909.

93. *Id.* at 908.

94. *Chatrie*, 136 F.4th at 103.

95. See *United States v. Rhine*, 652 F. Supp. 3d 38, 67 (D.D.C. 2023) (quoting *Chatrie*, 590 F. Supp. 3d at 909) (“‘Once a user opts into Location History, Google is always collecting data and storing all of that data’ in the Sensorvault.”).

96. See *id.*; *Kyllo v. United States*, 533 U.S. 27, 34–35 (2001).

97. *Kyllo*, 533 U.S. at 33–35, 40 (holding that a search occurred when the government used a device to monitor radiation through a home's walls); see also *United States v. Karo*, 468 U.S. 705, 714–15 (1984) (concluding that a search occurred when the government monitored a beeper inside “a private residence, a location not open to visual surveillance”).

98. See Google Amicus Brief, *supra* note 4, at 10 (Location History data capable of estimating location within twenty meters and collects data continuously).

a home without physical intrusion, geofence searches allow law enforcement to do the same.⁹⁹

2. *The Third-Party Doctrine Does Not Apply to Geofence Warrants*

The third-party doctrine does not save geofence warrants.¹⁰⁰ The TPD originated from cases involving limited physical business records, such as phone records and bank records.¹⁰¹ However, as the Court in *Carpenter v. United States* recognized, the TPD has never been absolute—it does not automatically apply to modern digital location data for two reasons: (1) such data is in a “qualitatively different category” of information revealing highly sensitive details; and (2) its disclosure is not “meaningfully voluntary.”¹⁰²

First, Location History data is far more detailed and comprehensive than traditional records or even the CSLI in *Carpenter*.¹⁰³ CSLI only tracks a phone’s location when the phone connects to cell towers, but Location History data is a mix of GPS, Wi-Fi, and Bluetooth, and it can locate devices with meter-level accuracy every two minutes.¹⁰⁴ This level of tracking creates an exhaustive chronicle of movement, exceeding the intimate window that the Court found protected in *Carpenter*.¹⁰⁵

The difference is not only quantitative but qualitative. A single hour’s worth of Location History data can reveal morning routines inside a home, the route taken to work, lunch meetings at specific restaurants, afternoon medical appointments (including which floor of a clinic), attendance at political rallies or religious services, and returns to a private residence¹⁰⁶—the exact categories of sensitive information *Carpenter* held are protected by the Fourth Amendment.¹⁰⁷

Secondly, Location History data is not a third-party business record; rather, it is the user’s personal property.¹⁰⁸ In contrast to bank records or call logs that are usually involved in TPD cases, Google has pointed out that its

99. See *Kyllo*, 533 U.S. at 33–35.

100. See *United States v. Chatrie*, 136 F.4th 100, 129 (4th Cir. 2025) (Wynn, J., concurring) (“In sum, the third-party doctrine is wholly inadequate to defeat Chatrie’s reasonable expectation of privacy in Location History data traceable to him.”).

101. See *United States v. Miller*, 425 U.S. 435, 437–38 (1946) (bank records); *Smith v. Maryland*, 442 U.S. 735, 737, 740–42 (1979) (phone records).

102. *Carpenter v. United States*, 585 U.S. 296, 309, 314 (2018).

103. See Google Amicus Brief, *supra* note 4, at 10.

104. *Id.*

105. See *Carpenter*, 585 U.S. at 297, 311, 314 (describing CSLI as creating an “exhaustive chronicle” providing an “intimate window into a person’s life”).

106. See *United States v. Rhine*, 652 F. Supp. 3d 38, 67 (D.D.C. 2023) (quoting *United States v. Chatrie*, 590 F. Supp. 3d 901, 909 (E.D. Va. 2022), *aff’d en banc*, 107 F.4th 319 (4th Cir. 2024), *aff’d on reh’g*, 136 F.4th 100 (4th Cir. 2025), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026)).

107. See *Carpenter*, 585 U.S. at 314.

108. See Google Amicus Brief, *supra* note 4, at 6.

location history feature is designed for the user's benefit.¹⁰⁹ Google has explained that this feature is the user's journal, which automatically records the trips the user takes and the places the user visits.¹¹⁰ Users, by turning on this feature, are allowed to enjoy services like travel summaries, location-based reminders, and suggestions that are based on the places they have been.¹¹¹ In this case, Google is more like a bailee who is holding data in trust for the user than a business that is generating its own transactional records.

Even if Location History data were to be considered as data "shared" with Google, *Carpenter* clearly states that the voluntariness inquiry does not end with that initial opt-in.¹¹² The Court recognized that "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."¹¹³ The same logic applies with even greater force to location services. The reason enabling location tracking features is necessary to use navigation apps, ride-sharing services, weather forecasts, and countless other applications is because they are part of basic necessities contemporary life requires.¹¹⁴

In the same way, the design of Google's interface refutes the idea of an informed, voluntary consent.¹¹⁵ When a user opens an app, the company prompts them to enable location tracking, whereas the privacy aspects are provided in long terms of service and hidden behind complex settings menus.¹¹⁶ In fact, once allowed, the tracking is done automatically and continuously, and the user has very limited and obscure options to turn it off.¹¹⁷ As Justice Sotomayor pointed out in *Jones*, and as Judge Wynn

109. *Id.* at 1.

110. *Id.* at 1.

111. *Id.* at 6–7.

112. *See Carpenter*, 585 U.S. at 314–15 (rejecting the third-party doctrine rationale of voluntary exposure for CSLI because it is not truly "shared").

113. *Id.* at 315 (quoting *Riley v. California*, 573 U.S. 373, 385 (2014)); *see also* *United States v. Smith*, 110 F.4th 817, 835 (5th Cir. 2024) (applying *Carpenter*'s "indispensable" rationale to Location History data).

114. *See United States v. Chatrle*, 136 F.4th 100, 127 (4th Cir. 2025) (Wynn, J., concurring) (noting location history is used for traffic updates and is an example of services that have become "indispensable to participation in modern society").

115. *See Smith*, 110 F.4th at 835–36 (stating opt-in processes "are hardly informed," and citing to Google employee comments stating that disabling it is "difficult enough that people won't figure it out") (internal quotations omitted); *see also* *United States v. Chatrle*, 590 F. Supp. 3d 901, 936 (E.D. Va. 2022), *aff'd en banc*, 107 F.4th 319 (4th Cir. 2024), *aff'd on reh'g*, 136 F.4th 100 (4th Cir. 2025), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026) (finding Google's privacy warnings are "limited and partially hidden" and "less than pellucid").

116. *See Chatrle*, 590 F. Supp. 3d at 909 (finding Google repeatedly prompts users to opt in to location history "multiple times across multiple apps").

117. *See id.* at 908–09, 913 (finding location history is "always collecting" data, and the process to delete data "[feels] like it is designed to make [deleting Location History] possible, yet difficult enough that people won't figure [it] out").

emphasized in his *Chatrie* opinion, these circumstances do not represent the knowing and voluntary disclosure that the TPD demands.¹¹⁸

Because geofence warrants require disclosure of highly sensitive, continuously collected, user-controlled location data—which is not similar to traditional third-party records nor shared voluntarily—they are an intrusion into protected Fourth Amendment interests.¹¹⁹ The TPD is not applicable here, and individuals have a reasonable expectation of privacy concerning the digital record of their movements.¹²⁰ Therefore, geofence searches are Fourth Amendment searches that require not just a warrant but one that is supported by particularized probable cause.¹²¹

B. Suspicion by Proximity: The Collapse of Probable Cause in Geofence Warrants

Geofence warrants are violations of the Fourth Amendment because they lack probable cause, and therefore, authorize searches that do not individually show that evidence of the crime will be found in the data of the particular device searched.¹²² The Fourth Amendment requires that “no Warrants shall issue, but upon probable cause,”¹²³ a standard that requires a “fair probability that contraband or evidence of a crime will be found in a particular place,” based on the totality of the circumstances.¹²⁴ In light of this, the Fourth Amendment demands answers to two questions: (1) whether there is probable cause to believe that a crime has been committed, and (2) whether the evidence of that crime is likely to be found in the specified place or on

118. See *United States v. Jones*, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring) (questioning whether disclosure to third parties in the digital age should defeat privacy expectations); *Chatrie*, 136 F.4th at 127 (Wynn, J., concurring) (stating that the voluntariness factor “does not tip decisively” and relying on the deceptive nature of opt-in processes and the indispensable nature of services).

119. See *Carpenter v. United States*, 585 U.S. 296, 311 (2018) (stating location data provides “an intimate window into a person’s life,” revealing “familial, political, professional, religious, and sexual associations”) (internal quotations omitted); see also *Chatrie*, 590 F. Supp. 3d at 907 (holding Location History data is the “most sweeping, granular, and comprehensive tool” for collecting location data).

120. See *Chatrie*, 590 F. Supp. 3d at 936 (concluding single tap to enable location history “likely do[es] not constitute a full assumption of the attendant risk of permanently disclosing one’s whereabouts”); *United States v. Smith*, 110 F.4th 817, 835–36 (5th Cir. 2024) (agreeing opt-in procedures can hardly be considered wholly informed and voluntary). But cf. *Chatrie*, 136 F.4th at 140 (Richardson, J., concurring) (arguing opting in to location history is voluntary because it requires an affirmative act and is not indispensable to modern society).

121. See U.S. CONST. amend. IV; see also *Chatrie*, 136 F.4th at 144 (Berner, J., concurring) (holding the government conducted a search when it acquired non-anonymous Location History data, which requires particularized probable cause).

122. U.S. CONST. amend. IV; see *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

123. U.S. CONST. amend. IV.

124. See *Gates*, 462 U.S. at 238.

the person to be searched.¹²⁵ These questions make sure that warrants do not authorize exploratory rummaging but are tethered to specific, articulated facts justifying the intrusion.¹²⁶

Geofence warrants fail to meet this standard. Far from relying on individualized suspicion, they hinge entirely on geographic proximity as a substitute for criminal involvement.¹²⁷ They do not rely on individualized suspicion, and yet they authorize searches of hundreds or thousands of individuals based solely on their presence in a defined area.¹²⁸ This replacement turns the probable cause requirement around and chooses investigative convenience over Fourth Amendment rights.

I. Being Near the Scene Is Not Enough

Geofence warrants are obtained when law enforcement knows the location and time of a crime but not the identity of the perpetrator.¹²⁹ In practice, this means the warrant authorizes Google to search the location data of numerous individuals without any specific reason to suspect any particular individual had any connection to that crime.¹³⁰

The government frequently defends geofence warrants by arguing that evidence of the unknown suspect's movements will inevitably be stored in Google's databases, given the ubiquity of smartphones in the modern era.¹³¹ While this idea is true, it completely ignores the deeper constitutional question.¹³² As the court noted in *Pharma II*, the probable cause analysis does not stop at the broad possibility of discovering the suspect's data.¹³³ Law enforcement must demonstrate not only a nexus to the unidentified offender

125. See *Zurcher v. Stanford Daily*, 436 U.S. 547, 554 (1978) (stating warrants may be issued to search “any property . . . at which there is probable cause to believe that fruits, instrumentalities, or evidence of a crime will be found”).

126. See *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971) (condemning “general, exploratory rummaging”).

127. See *United States v. Chatrie*, 590 F. Supp. 3d 901, 930–31 (E.D. Va. 2022), *aff’d en banc*, 107 F.4th 319 (4th Cir. 2024), *aff’d on reh’g*, 136 F.4th 100 (4th Cir. 2025), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026) (rejecting proximity as proxy for suspicion in geofence context); see also *United States v. Smith*, 110 F.4th 817, 824–25 (5th Cir. 2024) (finding geofence warrants substitute mere proximity for individualized suspicion).

128. See *Chatrie*, 590 F. Supp. 3d at 931 (noting sweeps of numerous individuals without any specific reason to suspect those specific individuals).

129. See *United States v. Davis*, 109 F.4th 1320, 1328 (11th Cir. 2024) (showing how geofence warrants are particularly useful when investigators know the location and time of a crime but cannot identify a suspect).

130. See *Chatrie*, 590 F. Supp. 3d at 915–19 (geofence warrants sweep location data from bystanders).

131. See, e.g., *id.* at 906–07 (providing one example of the government obtaining a geofence warrant, “whose use has grown exponentially in recent years”); *Smith*, 110 F.4th at 822 (demonstrating increasing government reliance on “sweeping searches of . . . location databases” where identities of suspects are unknown).

132. See *Pharma II*, 481 F. Supp. 3d 730, 748 (N.D. Ill. 2020).

133. *Id.*

but also a justification for rifling through the intimate information of innocent bystanders whose data will be indiscriminately swept up.¹³⁴

To authorize a search of everyone within a defined area, an officer must have probable cause to believe every person in that place was involved in or witnessed the criminal activity.¹³⁵ However, when looking at geofence warrants, it is impossible to show that probable cause existed because officers do not know who was present at the scene.¹³⁶

This approach resurrects and rebrands the “mere propinquity” reasoning that the Supreme Court rejected in *Ybarra v. Illinois*.¹³⁷ There, police obtained a warrant to search a tavern and its bartender for drugs.¹³⁸ When officers arrived, they frisked every patron in the bar, claiming each person’s presence in the tavern created suspicion.¹³⁹ The Court held this search as unconstitutional, finding that “a person’s mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person.”¹⁴⁰ Geofence warrants are based on this exact logic; they repaint brick-and-mortar taverns to digital spaces, substituting latitude and longitude for physical doorways.¹⁴¹ Nevertheless, the constitutional violation that the Court found in *Ybarra* remains the same.¹⁴²

134. See *United States v. Brown*, No. 1:16-CR-427-AT-JKL-31, 2025 WL 1674283, at 1*4 (N.D. Ga. June 13, 2025) (expressing “alarm at the Government’s widespread use of geofence warrants to drum up suspects out of thin air in the absence of other evidence,” noting it “runs counter to deeply rooted Fourth Amendment principles”); see also *Pharma II*, 481 F. Supp. 3d at 749 (requiring a nexus between an unidentified offender and limits on bystander intrusion).

135. See *United States v. Chatrie*, 136 F.4th 100, 153 (4th Cir. 2025) (Berner, J., concurring); see also *Ybarra v. Illinois*, 444 U.S. 85, 86, 91 (1979) (“[A] person’s mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person.”).

136. See *Smith*, 110 F.4th at 837 (search occurring while law enforcement officials “have no idea who they are looking for”); *United States v. Fuentes*, No. CR-21-358-RAW, 2024 WL 5494054, at *10 (E.D. Okla. Sep. 3, 2024) (law enforcement had reasonable suspicion a crime had been committed but “absolutely no showing in the Affidavit for Search warrant that Google held evidence of a crime in its Location History data since it had no idea who committed the crime”).

137. 444 U.S. 85, 91 (1979).

138. *Id.* at 87–88.

139. *Id.* at 88–89, 91.

140. *Id.* at 86.

141. See generally *United States v. Rhine*, 652 F. Supp. 3d 38, 66 (D.D.C. 2023) (discussing the use of geofence warrants when the location or identity of the suspect is unknown).

142. See *United States v. Chatrie*, 590 F. Supp. 3d 901, 933 (E.D. Va. 2022), *aff’d en banc*, 107 F.4th 319 (4th Cir. 2024) *aff’d on reh’g*, 136 F.4th 100 (4th Cir. 2025), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026) (holding the *Ybarra* precedent demands more than mere propinquity to crime).

2. The “Inverted Probable Cause” Problem

Courts have rightly called geofence warrants an “inverted probable cause argument.”¹⁴³ Traditionally, warrants move from specific to general; officers identify a suspect with evidence, then seek a warrant targeting that suspect’s records.¹⁴⁴ Geofence warrants flip that order.¹⁴⁵ Prosecutors and detectives start with a generalized belief that someone in an area committed a crime, then use that belief to justify a broad fishing expedition through everyone’s data in the area.¹⁴⁶ This inversion corrodes the probable cause requirement. When the magistrate approves a geofence warrant, the court authorizes data collection from vast numbers of people (often numbering in the hundreds or thousands) who were simply in the wrong place at the wrong time.¹⁴⁷ The sheer volume of unconnected information collected by these warrants only serves to dilute the government’s probable cause showing because the probability of discovering the true culprit diminishes when it is buried beneath the noise of irrelevant entries.¹⁴⁸

Moreover, the Supreme Court has held that warrants that authorize searches of “all persons” in a particular area are valid only when there is probable cause to believe all persons present are involved in the criminal activity.¹⁴⁹ Because geofences generally cover areas that are densely populated, such as residences, businesses, and public spaces, the government cannot credibly make that showing.¹⁵⁰

3. Systematic Overbreadth: Evidence from the Real World

This problem is systemic. The ACLU of Northern California released an investigative report, which reviewed a large number of geofence warrants

143. *Id.* (rejecting the government’s “inverted probable cause argument” as unpersuasive); *see also* *Chatrie*, 136 F.4th at 155 n.42 (finding that a warrant was invalid due to an inverted probable cause argument).

144. *See* *United States v. Smith*, 110 F.4th 817, 822 (5th Cir. 2024).

145. *Id.*

146. *See id.* at 837 (describing geofences as enabling “fishing expedition[s]”).

147. *See, e.g.*, *United States v. Fuentes*, No. CR-21-358-RAW, 2024 WL 5494054, at *3–5 (E.D. Okla. Sep. 3, 2024) (including geofence captured data from numerous devices); *In re Search of Info. That is Stored at the Premises Controlled by Google, LLC*, 542 F. Supp. 3d 1153, 1157 (D. Kan. 2021) (highlighting a large amount of data included individuals not involved in the alleged criminal activity).

148. *See In re Search of Info. That is Stored at the Premises Controlled by Google, LLC*, 542 F. Supp. 3d at 1157.

149. *See Owens ex rel. Owens v. Lott*, 372 F.3d 267, 276 (4th Cir. 2004); *United States v. Chatrie*, 590 F. Supp. 3d 901, 930 (E.D. Va. 2022), *aff’d en banc*, 107 F.4th 319 (4th Cir. 2024), *aff’d on reh’g*, 136 F.4th 100 (4th Cir. 2025), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026); *see Pharma II*, 481 F. Supp. 3d 730, 751 (N.D. Ill. 2020); *see also* *United States v. Guadarrama*, 128 F. Supp. 2d 1202, 1211 (E.D. Wis. 2001) (applying case law requiring probable cause).

150. *See* Jake Snow, *Cops Blanketed San Francisco in Geofence Warrants. Google Was Right to Protect People’s Privacy*, ACLU N. CAL. (Jan. 7, 2024), <https://www.aclunorcal.org/news/cops-blanketed-san-francisco-geofence-warrants-google-was-right-protect-peoples-privacy/> [<https://perma.cc/EUG5-786Z>].

in San Francisco from January 2018 to August 2021.¹⁵¹ The report found that these warrants were not targeted searches but rather the warrants “blanketed” the city, thereby collecting data from one hundred twenty-one private homes; eighty-two apartment buildings; eighty-four workplaces (including tech firms like Oracle); thirty-two bars and restaurants; twelve places of worship (such as mosques and churches); seven medical sites (like Kaiser Permanente clinics); five grocery stores; and even seven schools and daycares.¹⁵² These findings show that geofence warrants invade private spaces and collect data without effective consent.¹⁵³ Prioritizing investigative convenience over constitutional safeguards chills freedoms and disproportionately harms communities already heavily policed.¹⁵⁴

4. The Multi-Step Structure Amplifies the Probable Cause Deficiency

Geofence searches typically proceed in staged steps, and that structure exacerbates the constitutional problem.¹⁵⁵ The Fourth Amendment requires probable cause to exist at the time of the warrant application, not to be added later after searches have begun.¹⁵⁶ However, geofence warrants routinely use a three-step process where the magistrate approves a broad data pull up front, and then agents narrow the results in subsequent, unsupervised stages.¹⁵⁷ At the moment of application, detectives cannot credibly show probable cause for the later narrowing.¹⁵⁸ The initial sign-off, therefore, becomes a blank check that future, extra-judicial filtering will attempt to justify.¹⁵⁹

A single warrant that allows broader follow-up searches of any kind is against fundamental Fourth Amendment principles.¹⁶⁰ It is not possible to create probable cause after the fact; however, geofence warrants allow for more invasive searches with each step, without requiring the officer to return

151. *Id.*

152. *Id.*

153. *Id.*

154. *Id.* (“[W]hen surveillance technology is used, it must be subject to public oversight [It] disproportionately targets marginalized communities . . . causing harm to people who are low-income or people of color.”).

155. *See* *United States v. Chatrie*, 136 F.4th 100, 153 (4th Cir. 2025) (Berner, J., concurring) (“Probable cause must be evaluated at the time of warrant application, not in light of subsequent developments.”).

156. *See* *Smith v. Munday*, 848 F.3d 248, 253 (4th Cir. 2017).

157. *See* *Chatrie*, 136 F.4th at 145 (Berner, J., concurring) (noting a three-step process where the magistrate approves a broad data pull up front, then agents narrow results in subsequent, unsupervised stages).

158. *Id.* (“Consequently, at the time the Government applied for the geofence warrant, it could not have explained the specific rationale that would ultimately support its second and third requests.”).

159. *Id.*

160. *See id.* at 155 (Berner, J., concurring) (discussing the view that the search violated the Fourth Amendment because the government lacked probable cause for increasingly intrusive searches at Steps Two and Three).

to a magistrate judge.¹⁶¹ The final outcome is a system where the first judicial authorization serves as a shield against these subsequent, unjustified privacy invasions that no neutral and detached judge ever approved.¹⁶²

Geofence warrants fail the probable cause requirement in every realm. They substitute proximity for individualized suspicion, invert the traditional relationship between evidence and search authorization, systematically sweep up the data of innocent bystanders, and delegate critical probable cause determinations to officers and Google.¹⁶³ No reasonable interpretation of the Fourth Amendment can allow warrants that authorize searching potentially thousands of people based solely on their location, without any particular reason to believe any specific individual possesses evidence of a crime.¹⁶⁴

C. A Warrant Without Particularity: When No One Knows Who or What Is Being Searched

The Fourth Amendment stipulates that the warrants “particularly describ[e] the place to be searched, and the persons or things to be seized.”¹⁶⁵ This requirement serves to confirm that the searches are carefully tailored to probable cause,¹⁶⁶ and to stop law enforcement from having a free-for-all in deciding what to search or seize.¹⁶⁷ A warrant that gives complete discretion to the executing officer is invalid on its face.¹⁶⁸

Geofence warrants fail this particularity requirement for two reasons. First, they compel providers like Google to conduct indiscriminate searches through the location histories of hundreds of millions of users, without describing any particular suspect or device to be identified.¹⁶⁹ Second, they grant law enforcement unlimited discretion to decide which anonymized accounts to investigate further, and whose identities to unmask, without

161. See *id.* at 153 (citing *Munday*, 848 F.3d at 253) (“Probable cause must be evaluated at the time of the warrant application, not in light of subsequent developments.”); *id.* at 155 (Berner, J., concurring) (finding it impossible for a detective to describe facts supporting the decision to conduct a Fourth Amendment search targeting specific individuals when he applied for the initial warrant).

162. *Id.* at 155.

163. See *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979); *United States v. Smith*, 110 F.4th 817, 837 (5th Cir. 2024) (noting initial Step One search requires Google to “search[] through the entirety of its Sensorvault,” allowing “general, exploratory rummaging”).

164. See *Smith*, 110 F.4th at 837.

165. U.S. CONST. amend. IV.

166. See *Smith*, 110 F.4th at 830.

167. See *Groh v. Ramirez*, 540 U.S. 551, 561 (2004) (requirement assures the individual of “limits of [the officer’s] power to search”); see also *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971) (particularity prevents “general, exploratory rummaging”).

168. *Stanford v. Texas*, 379 U.S. 476, 485 (1965).

169. See *Smith*, 110 F.4th at 824 (for every geofence warrant, Google “must search each account in its entire Sensorvault—all 592 million—to find responsive user records.”).

objective criteria or renewed judicial oversight.¹⁷⁰ These deficiencies render geofence warrants modern versions of the general warrants and writs of assistance that the Framers sought to prohibit with the Fourth Amendment.¹⁷¹

Courts have described geofence warrants as uncomfortably akin to the “reviled ‘general warrants’ and ‘writs of assistance’ of the colonial era.”¹⁷² Historically, general warrants authorized searches based on suspicion that some offense had occurred, leaving the executing officer discretion to decide whom to search and what to seize.¹⁷³ This structure should sound familiar because many geofence warrant applications rely on the same vague assertion that “a crime was committed” without describing with particularity the individual or item to be searched.¹⁷⁴ As a result, the provider is directed to “rummage through troves of location data from hundreds of millions of Google users without any description of the particular suspect or suspects to be found.”¹⁷⁵ This sweeping initial search is itself constitutionally deficient.¹⁷⁶ Like colonial general warrants, which allowed broad exploratory intrusions justified only by a general offense, Step One orders Google to scan vast swaths of data for potential evidence.¹⁷⁷

A warrant must limit the ability to search “to the specific areas and things for which there is probable cause to search,” ensuring the search is “carefully tailored to its justifications[.]”¹⁷⁸ The particularity requirement means that nothing should be left to the discretion of the officer executing the warrant.¹⁷⁹ Geofence warrants fail this requirement. During Step One, law enforcement compels Google to search its entire Sensorvault database, which contains location data for over 500 million users, to identify devices within

170. See *People v. Meza*, 312 Cal. Rptr. 3d 1, 16 (Cal. Ct. App. 2023) (finding the warrant invalid because it “fail[ed] to place any meaningful restriction on the discretion of law enforcement officers to determine which accounts would be subject to further scrutiny or deanonymization”).

171. See *Smith*, 110 F.4th at 836.

172. *Id.* at 836 (quoting *Riley v. California*, 573 U.S. 373, 403 (2014)); *Wells v. State*, 714 S.W.3d 614 (Tex. Crim. App. 2024) (Finley, J., concurring); see generally Shelby Stender, *Circumventing the Fourth Amendment: The Unconstitutional Nature of Geofence Warrants*, 2024 UTAH L. REV. 733 (2024) (noting that the Fourth Amendment was created to end rummaging in search of evidence).

173. *Smith*, 110 F.4th at 826; *United States v. Brown*, 828 F.3d 375, 383 (6th Cir. 2016); see also *United States v. Fuentes*, No. CR-21-358-RAW, 2024 WL 5494054, at *8 (E.D. Okla. Sep. 3, 2024) (providing an example of an officer acting on reasonable suspicion).

174. *Fuentes*, 2024 WL 5494054, at *10 (“[L]aw enforcement had a reasonable suspicion that a crime had been committed at a particular location but absolutely no showing in the Affidavit for Search warrant that Google held evidence of a crime in its Location History data since it had no idea who committed the crime.”).

175. *Smith*, 110 F.4th at 837–38.

176. *Id.* at 820 (holding Step One unconstitutional for lack of particularity).

177. See *Stanford v. Texas*, 379 U.S. 476, 480 (1965) (describing general warrants as enabling broad searches without specificity); see also *Smith*, 110 F.4th at 826 (analogizing geofences to general warrants for their exploratory nature).

178. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

179. *Stanford*, 379 U.S. at 485.

the geofence.¹⁸⁰ The warrant does not identify any suspects nor specific devices to be located.¹⁸¹ It provides only time and geographic boundaries and instructs Google to find everyone who was there.¹⁸²

This is not particularity; it is the exact blanket authority that the Fourth Amendment condemns.¹⁸³ The warrant transforms Google into an investigative arm of the government, forcing the company to probe through hundreds of millions of private location records to generate leads for law enforcement.¹⁸⁴ The fact that Google performs the initial search does not exempt it from Fourth Amendment constraints, especially when it is the government compelling it to search user data pursuant to a warrant.¹⁸⁵ In this case, Google (or the entity) acts as the government's agent, and the search must comply with constitutional requirements.¹⁸⁶

Moreover, temporal and geographic limitations cannot cure a warrant's lack of particularity when it otherwise grants discretion to decide who or what to seize.¹⁸⁷ As the Northern District of Illinois explained in *Pharma II*, a warrant cannot satisfy the Fourth Amendment just by adding time and location restrictions if it otherwise grants the government discretion to decide what or whom to seize.¹⁸⁸ The warrant must identify its targets with sufficient specificity that executing officers, or, in this case, technology companies acting as government agents, have objective criteria to guide their discretion.¹⁸⁹

At Steps Two and Three, the situation becomes even worse as constitutional rights are violated and law enforcement officers are given complete freedom to exercise their discretion in the most intrusive stages of the search without any judicial limitation.¹⁹⁰ After receiving the anonymized list from Step One, the officers alone decide which devices look "relevant" and deserve further investigation, what additional location data to be

180. See *Smith*, 110 F.4th at 824 (noting that for every geofence warrant, Google "must search each account in its entire Sensorvault—all 592 million—to find responsive user records"); *United States v. Brown*, No. 1:16-CR-427-AT-JKL-31, 2025 WL 1674283, at *6 (N.D. Ga. June 13, 2025) ("Google is always collecting data and storing *all* of that data in the Sensorvault.").

181. See *United States v. Rhine*, 652 F. Supp. 3d 38, 66 (D.D.C. 2023) (explaining that geofence warrants are used "when the crime location is known but the identities of suspects is not[]").

182. *Id.*

183. *Brown*, 2025 WL 1674283, at *5.

184. See *United States v. Fuentes*, No. CR-21-358-RAW, 2024 WL 5494054, at *10 (E.D. Okla. Sep. 3, 2024) (stating that a search required in Step One "is the hallmark of a general warrant—aimless searching with only the hope that the result will justify the means[]").

185. See *Smith*, 110 F.4th at 838 n.12 ("Google's actions, including at Step 1, are 'conducted in response to legal compulsion'" and Google acts as an "instrument or agent of the Government").

186. *Id.*

187. *Pharma II*, 481 F. Supp. 3d 730, 748 (N.D. Ill. 2020).

188. *Id.* at 754.

189. *Id.*

190. See *People v. Meza*, 312 Cal. Rptr. 3d 1, 15 (Cal. Ct. App. 2023) (finding geofence warrant gave law enforcement unbridled discretion); see also *Smith*, 110 F.4th at 825–26 (explaining law enforcement's freedom as it relates to on-the-job decision making).

requested for those devices, what geographic area that new tracking should cover, how much time that tracking should span, and which accounts should ultimately be unmasked.¹⁹¹ None of these decisions are governed by objective standards, and none of these decisions are approved by a neutral and detached judge.¹⁹² Instead, the warrant does not specify any criteria for relevance, any limits on geographic expansion, nor any threshold requirements for de-anonymization.¹⁹³ Officers go through the list and choose whom to investigate based on their own subjective judgment.¹⁹⁴

IV. THE GOOD-FAITH EXCEPTION SHOULD NOT APPLY TO GEOFENCE WARRANT SEARCHES

The Court has identified four exceptions to *Leon*'s good-faith exception.¹⁹⁵ *Leon* recognizes exceptions to the good-faith rule: (1) the affidavit contains knowingly or recklessly false statements; (2) the magistrate wholly abandoned the judicial role; (3) the affidavit is so lacking in indicia of probable cause that belief in its validity is unreasonable; or (4) the warrant is so facially deficient in its description of the place to be searched or the things to be seized that officers cannot reasonably presume it valid.¹⁹⁶

A. Magistrate Approval of Geofence Warrants Reflects a Structural Breakdown of Judicial Oversight

The *Leon* good-faith exception applies when the failure occurs from the magistrate.¹⁹⁷ Under *Leon*, evidence should not be suppressed when law enforcement officers reasonably rely on a neutral magistrate's judgment.¹⁹⁸ This is based on the fact that excluding evidence because of a magistrate's error alone is insufficient to deter similar misconduct, because magistrates are considered "neutral judicial officers" with "no stake in the outcome of particular criminal prosecutions."¹⁹⁹ But when magistrates approve geofence warrants that delegate probable cause determinations to law enforcement and

191. See *In re Search of Info. That is Stored at the Premises Controlled by Google, LLC*, 542 F. Supp. 3d 1153, 1159 (D. Kan. 2021) (finding ability to unilaterally tell Google which cell phones the officer wanted to unmask to obtain the owner's personal information was granting law enforcement judicial discretion).

192. See *Meza*, 312 Cal. Rptr. 3d at 16 (finding warrant invalid because it "fail[ed] to place any meaningful restriction on the discretion of law enforcement officers to determine which accounts would be subject to further scrutiny or deanonymization").

193. *Id.*

194. *Id.*

195. See *United States v. Leon*, 468 U.S. 897, 923 (1984).

196. See *id.* at 923.

197. See *id.* at 917 (explaining that the exclusionary rule is designed to deter police misconduct, and excluding evidence due to a magistrate's error alone is insufficient to deter similar misconduct).

198. *Id.* at 922.

199. *Id.* at 917.

private corporations, the constitutional safeguard collapses.²⁰⁰ What remains is not judicial oversight, it is judicial abdication.

The Fourth Amendment protects United States citizens from unreasonable searches and seizures by requiring that a neutral and detached judge issue a search warrant.²⁰¹ Yet this shield is corroded when magistrate judges issue these three-step warrants without requiring judicial reapproval at each stage.²⁰² Approved geofence warrants that permit Steps Two and Three (more invasive searches) to be conducted without judicial review are judicial error because the magistrate allows inherently more invasive searches to occur outside the court's supervision.²⁰³

1. Magistrate Judges Giving Judicial Power to a Private Corporation Is the Magistrate Judge Abandoning Their Role

It is easy to get distracted and attempt to pinpoint which step in the Google process constitutes an invasion of privacy. However, regardless of which step is deemed to be the critical point of intrusion, probable cause determinations cannot be delegated to private entities.²⁰⁴ By approving a particularity evaluation to be done by law enforcement and Google, the magistrate judges delegate their constitutional duty to a private party.²⁰⁵ This structure improperly grants law enforcement unbridled discretion to determine which accounts are subject to further intrusion.²⁰⁶

200. See *United States v. Chatrie*, 136 F.4th 100, 159 (4th Cir. 2025) (Gregory, J., dissenting) (noting warrant “ceded authority and decision-making from an independent judicial officer to a private corporation”).

201. See U.S. CONST. amend. IV; *Dalia v. United States*, 441 U.S. 238, 255 (1979).

202. See *United States v. Chatrie*, 590 F. Supp. 3d 901, 927 (E.D. Va. 2022), *aff’d en banc*, 107 F.4th 319 (4th Cir. 2024), *aff’d on reh’g*, 136 F.4th 100 (4th Cir. 2025), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026) (Steps Two and Three were “undertaken with no judicial review whatsoever”); *People v. Meza*, 312 Cal. Rptr. 3d 1, 25 n.11 (Cal. Ct. App. 2023) (judicial oversight at Steps 2 and 3, “not just prior to issuance of the warrant, would resolve many of the constitutional deficiencies[]”).

203. See *Chatrie*, 590 F. Supp. 3d at 927; *Meza*, 312 Cal. Rptr. 3d at 25 n.11.

204. See *Chatrie*, 136 F.4th at 155 (Berner, J., concurring) (“Probable cause determinations cannot be delegated to private entities.”); *Birchfield v. North Dakota*, 579 U.S. 438, 469 (2016) (search warrants “ensure that a search is not carried out unless a neutral magistrate makes an independent determination that there is probable cause to believe that evidence will be found[]”).

205. See *Chatrie*, 136 F.4th at 155 (Berner, J., concurring) (detective failed to show probable cause for Steps Two and Three, and “[u]nder the terms of the geofence warrant, Google, not a magistrate, was the sole entity that could confine the scope of the ultimate search[]”).

206. See *Chatrie*, 590 F. Supp. 3d at 927, 934 (explaining that Steps Two and Three “improperly provided law enforcement and Google with unbridled discretion to decide which accounts will be subject to further intrusions[]” and “lack any semblance of objective criteria to guide how officers would narrow the lists of users”); see, e.g., *In re Search of Info. That Is Stored At the Premises Controlled by Google LLC*, 579 F. Supp. 3d 62, 88 (D.D.C. 2021) (rejecting a geofence warrant protocol that granted law enforcement unbridled discretion to obtain identifying information without judicial oversight); *Pharma II*, 481 F. Supp. 3d 730, 754 (N.D. Ill. 2020) (finding a geofence warrant violated the particularity requirement because it left officers with unbridled discretion); *Meza*, 312 Cal. Rptr. 3d at 14–16 (holding

By delegating key judicial functions to Google, the magistrate judge abandons the “neutral and detached” role required by the Fourth Amendment.²⁰⁷ The warrant process has been converted from a judicial act to a simple administrative action. It is Google, not a magistrate judge, which decides what data to disclose and when.²⁰⁸ Here, the magistrate does not interpret or limit the warrant’s reach. Rather, the magistrate signs off and allows Google to perform the very constitutional balancing the court is supposed to do.²⁰⁹

This delegation crosses a constitutional line.²¹⁰ While *Lo-Ji Sales v. New York* condemned a magistrate judge who became too involved in an investigation, the Fourth Amendment violation there, and here, stems from the same root defect: the loss of judicial neutrality.²¹¹ The *Lo-Ji* magistrate corrupted the process through overreach;²¹² a geofence magistrate corrupts it through abdication.²¹³ Both acts destroy the separation between executive and judicial roles that the Fourth Amendment was designed to protect.²¹⁴

In *Lo-Ji*, the judge joined law enforcement in executing a search and crossed the judicial boundary by acting as an investigator.²¹⁵ A magistrate judge, in the geofence warrant situation, also crosses the same line by becoming a sideline observer.²¹⁶ In authorizing a private party—Google—to perform constitutional functions on the court’s behalf, the judge abandons their role.²¹⁷ The result is fundamentally identical; the magistrate ceases to act as a neutral arbiter and instead becomes part of the investigation, whether by participation or by passivity.²¹⁸ The Fourth Amendment should not

a geofence warrant violated the particularity requirement where officers had unbridled discretion to decide which account would be subject to further scrutiny or deanonymization).

207. See *In re Search of One Device and Two Individuals Under Rule 41*, 783 F. Supp. 3d 183, 187 (D.D.C. 2025) (a magistrate judge must “perform his ‘neutral and detached’ function and not serve merely as a rubber stamp for the police”).

208. See *Chatrie*, 136 F.4th at 155 (Berner, J., concurring) (under the warrant’s terms, “Google, not a magistrate, was the sole entity that could confine the scope of the ultimate search[]”).

209. *Id.*

210. See *id.*

211. See *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 326–27 (1979) (holding a magistrate who fails to manifest neutrality and detachment demanded of a judicial officer cannot provide valid authorization for otherwise unconstitutional search).

212. See *id.* at 327 (explaining that the magistrate became “a member, if not the leader, of the search party which was essentially a police operation”).

213. See *Chatrie*, 136 F.4th at 157 (Gregory, J., dissenting).

214. See U.S. CONST. amend. IV; *Dalia v. United States*, 441 U.S. 238, 255 (1979).

215. See *Lo-Ji Sales, Inc.*, 442 U.S. at 327.

216. See *Chatrie*, 136 F.4th at 155 (Berner, J., concurring).

217. See *United States v. Chatrie*, 590 F. Supp. 3d 901, 934 (E.D. Va. 2022), *aff’d en banc*, 107 F.4th 319 (4th Cir. 2024), *aff’d on reh’g*, 136 F.4th 100 (4th Cir. 2025), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026) (multi-step process improperly provided law enforcement and Google with “unbridled discretion to decide which accounts will be subject to further intrusions” and searches at Steps Two and Three were “undertaken with no judicial review whatsoever”).

218. See *United States v. Leon*, 468 U.S. 897, 923 (1984) (a magistrate must not “serve merely as a rubber stamp for the police”); *In re Search of One Device and Two Individuals Under Rule 41*, 783 F.

care how neutrality is lost, only that it is. Therefore, a magistrate who relinquishes control to a third party has wholly abandoned the judicial role in the same way as one who joins the police on a search.²¹⁹

2. Magistrate Judges Rubberstamping Geofence Warrants Is an Error and Leaves a Powerless Corporation in Charge

A magistrate fails to perform the duties of a neutral and detached magistrate when reviewing geofence applications because the magistrate acts as nothing more than a rubber stamp for the police.²²⁰ In *Chatrie*, the magistrate did not ask a single question and made no changes to the warrant before signing off on a sweeping and intrusive search.²²¹ The issue of insufficient judicial oversight in the case of geofence warrants is just the tip of the iceberg. Research has shown that judges, on average, spend less than three minutes reviewing a warrant application.²²² This speed of review, combined with the intricate nature of geofence data, points to the failure of the whole system to provide carefully considered, impartial judgment.²²³ The result is a process that appears judicial but, beneath the surface, is automatic—resulting in the quiet erosion of the Fourth Amendment’s most basic safeguard.

Furthermore, this delegation of probable cause analysis to Google does not give Google any power to prevent overzealous law enforcement.²²⁴ Google’s three-step process is not a binding law.²²⁵ Under current practice, Google’s three-step process is often ignored or curtailed.²²⁶ Some magistrate

Supp. 3d 183, 194 (D.D.C. 2025) (“The court’s credibility is based on a belief in its neutrality. But how can a court that never says ‘no’ be neutral?”).

219. See *Leon*, 468 U.S. at 923 (showing an example of a magistrate who “wholly abandoned his judicial role” and the exception to good-faith rule); *Lo-Ji Sales, Inc.*, 442 U.S. at 326–27; *United States v. Wilhelm*, 80 F.3d 116, 121 (4th Cir. 1996).

220. See *Leon*, 468 U.S. at 914 (“[A] magistrate must purport to perform his neutral and detached function and not serve merely as a rubber stamp for the police.”).

221. See *Chatrie*, 590 F. Supp. 3d at 918 (noting the magistrate “asked no questions of [Detective] Hylton” and did not “seek to modify anything in the affidavit” even though this appeared to be the first geofence warrant application the magistrate had considered) (internal quotations omitted).

222. See Stender, *supra* note 172, at 756 (featuring a study in Salt Lake City that showed that out of approximately 8,400 electronic warrants brought to magistrate judge in one year, “more than half were approved in ten minutes or less[.]” and “[t]wo dozen were approved in less than one minute[.]”); RICHARD VAN DUIZEND, L. SUTTON & CHARLOTTE CARTER, *THE SEARCH WARRANT PROCESS: PRECONCEPTIONS, PERCEPTIONS, AND PRACTICES* 31 (1985).

223. See Stender, *supra* note 172, at 756 (problem of mass approval “is systemic”).

224. See *United States v. Chatrie*, 136 F.4th 100, 155 (4th Cir. 2025) (Bernier, J., concurring) (“Probable cause determinations cannot be delegated to private entities.”); *id.* at 161 (Gregory, J., dissenting) (discussing that constitutional rights “should not and cannot be defined by the internal policies of a private corporation[.]”).

225. See *GEOFENCE WARRANT PRIMER*, *supra* note 4, at 1–2.

226. See Google Amicus Brief, *supra* note 4, at 18 (“[L]aw enforcement can compel Google to provide additional contextual location coordinates beyond the time and geographic scope of the original request.”).

judges approve warrants that allow law enforcement to skip intermediate review altogether, leading to premature disclosure of identifying data.²²⁷ An example of this is seen in *United States v. Fuentes*, where the warrant application completely omits Step Two set out by Google, resulting in the revelation of Step Three information after the officer received the first broad, anonymized list.²²⁸ The magistrate, by failing to scrutinize the warrant and instead rubber-stamping the request, allowed the investigator to access the most intimate information that Google has about an innocent party.²²⁹

3. Although Not Dispositive, Magistrate Error Needs to Be Analyzed Nonetheless

To be clear, magistrate error alone does not automatically justify suppression; *Leon* makes that plain.²³⁰ But these errors cannot be dismissed as harmless when they fit squarely within the framework of *Leon*'s own exceptions.²³¹ The good-faith doctrine assumes that a neutral magistrate has exercised meaningful oversight and that the resulting warrant bears indicia of probable cause and particularity.²³² Where, as here, the magistrate's review is a performance, the warrant's foundation is so lacking in probable cause that no reasonable officer could rely on it, and its terms are so facially deficient that no one could presume it valid, *Leon*'s rationale collapses.²³³ In other words, judicial error may not stand alone, but when paired with a warrant this constitutionally hollow, suppression is not only warranted; it is required to preserve the integrity of the Fourth Amendment.²³⁴

227. *United States v. Fuentes*, No. CR-21-358-RAW, 2024 WL 5494054, at *4 (E.D. Okla. Sep. 3, 2024) (discussing the warrant that did not adhere to three-step process, "eliminating the anonymizing step" and leaving the matter "entirely up to law enforcement").

228. *Id.*

229. *Id.* ("Thornton immediately eliminated the person associated with the account ending in 008 because the individual stayed at the scene until law enforcement arrived. If the Search Warrant had followed the three-step process, this account would have likely been eliminated from the investigation without the revelation of the individual's personal information because the contextualized data would have been evaluated for the length of time the user stayed at the scene.").

230. See *United States v. Leon*, 468 U.S. 897, 917 (1984) (excluding evidence because of magistrate's error alone is insufficient to deter similar misconduct); see also *Herring v. United States*, 555 U.S. 135, 144 (2009) (explaining that the exclusionary rule applies only when police misconduct is sufficiently deliberate so that suppression would meaningfully deter it); *United States v. Chatrie*, 136 F.4th 100, 119 (4th Cir. 2025) (Wynn, J., concurring) ("As we know from *Leon*, the magistrate's errors alone are insufficient to warrant suppression of evidence obtained pursuant to a deficient warrant.").

231. See *Leon*, 468 U.S. at 923 (articulating four circumstances where the good-faith exception does not apply).

232. See *id.* at 922.

233. See *id.* at 923 (noting that the good-faith exception does not apply when "the issuing magistrate wholly abandoned his judicial role"); *Groh v. Ramirez*, 540 U.S. 551, 563 (2004) (holding that "no reasonable officer could believe that a warrant that plainly did not comply with [the particularity] requirement was valid[]").

234. See *Chatrie*, 136 F.4th at 160 (Gregory, J., dissenting) (concluding that the warrant was facially deficient and "[e]xclusion of the evidence is therefore appropriate here[]"); *United States v. Fuentes*, No.

B. Beyond the Four Corners: Geofence Warrants So Lacking in Probable Cause That No Reasonable Officer Could Rely on Them

Under *Leon*, suppression is mandatory when the supporting affidavit is “so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.”²³⁵ As demonstrated above, geofence warrants categorically fail to establish probable cause.²³⁶ From this point, the question shifts from asking whether probable cause exists to whether the deficiency is so severe and so obvious that no reasonable officer could believe the warrant is valid.²³⁷ Geofence warrants do not suffer from weak or marginal probable cause issues that might escape an officer’s notice.²³⁸ Rather, they are structured so that their constitutional deficiency is unmistakable to any trained law enforcement officer.²³⁹

1. The Rejection of Proximity-Based Suspicion Is Not New or Obscure

Fourth Amendment case law holds that physical proximity to a crime scene does not, by itself, amount to individualized suspicion.²⁴⁰ This concept is not new and has been a cornerstone of Fourth Amendment jurisprudence for nearly half a century, clearly laid out by the Court in *Ybarra v. Illinois*.²⁴¹

In *Ybarra*, the Supreme Court decided that a search warrant for a bar and its bartender did not permit law enforcement to frisk every patron present just because they were close to the suspected crime.²⁴² The Court’s holding is clear: “[A] person’s mere propinquity to others independently suspected of

CR-21-358-RAW, 2024 WL 5494054, at *6, *11 (E.D. Okla. Sep. 3, 2024) (holding that the affidavit lacked probable cause on its face, and “[t]his falls short of good faith and mandates the suppression of the evidence derived from the Google search[.]”).

235. *Leon*, 468 U.S. at 923 (Powell, J., concurring) (internal quotations omitted) (quoting *Brown v. Illinois*, 422 U.S. 590, 611 (1975)).

236. See *supra* Section III.B (discussing the lack of probable cause in geofence warrants).

237. See *Leon*, 468 U.S. at 923.

238. See *infra* Sections IV.B.1–2 (discussing probable cause issues with geofence warrants).

239. See *Chatrue*, 136 F.4th at 160 (Gregory, J., dissenting) (finding that the officer need not know the Judiciary’s view on new technology to know that the information in the warrant was insufficient, because “it was not unclear what the Constitution demands of all warrants”); *Leon*, 468 U.S. at 919 n.20 (presuming that officers have “reasonable knowledge of what the law prohibits”); *Fuentes*, 2024 WL 5494054, at *11 (affidavit was “completely lacking any facts to indicate that the perpetrator of the offense possessed a cell phone,” which mandated suppression because it fell short of good faith). But see *United States v. Smith*, 110 F.4th 817, 840 (5th Cir. 2024) (declining to suppress the evidence because investigators were utilizing “a cutting-edge investigative technique” with a “dearth of court precedent” to guide law enforcement, making reliance reasonable).

240. See *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979); see also *Maryland v. Pringle*, 540 U.S. 366, 371 (2003) (stating that probable cause demands “‘a reasonable ground for belief of guilt[.]’ . . . particularized with respect to the person to be searched or seized”).

241. See *Ybarra*, 444 U.S. at 88–89.

242. *Id.* at 88–89, 91.

criminal activity does not, without more, give rise to probable cause to search that person.”²⁴³

Nevertheless, geofence warrants keep repeating the same argument that the Court in *Ybarra* stated was not enough.²⁴⁴ They link suspicion to a device being inside a digital boundary, replacing the bar walls with GPS coordinates, and the result is the same constitutional problem.²⁴⁵ A reasonable officer, familiar with *Ybarra*, would recognize right away that a warrant allowing the search of hundreds or thousands of devices solely based on their presence is lacking that specific showing of probable cause that the Fourth Amendment and *Ybarra* demand.²⁴⁶

The government, therefore, cannot credibly argue that officers might not be aware of this principle.²⁴⁷ *Ybarra* is a landmark case. Its rejection of proximity-based searches appears in Fourth Amendment treatises, training materials, and countless judicial opinions.²⁴⁸ A reasonable officer knows, or should know, that this theory has been rejected for decades.²⁴⁹

2. *The Affidavits Supporting Geofence Warrants Are Filled with Boilerplate Language and Are Conclusory*

The *Ybarra* proximity issue is not the only structural flaw in geofence warrants. The supporting affidavits for these applications are packed with general assertions that do not make any case-specific connection between the requested data and the crime under investigation.²⁵⁰

243. *Id.* at 91.

244. *See Pharma II*, 481 F. Supp. 3d 730, 753 (N.D. Ill. 2020) (noting that the geofence warrant included persons “based on nothing other than their close proximity”).

245. *See id.*; *see also Ybarra*, 444 U.S. at 91.

246. *See In re Search of Info. Stored at Premises Controlled by Google*, No. KM-2022-79, 2022 WL 584326, at *7 (Va. Cir. Ct. Feb. 8, 2022) (“Imagine if, in *Ybarra*, police knew someone in the bar possessed heroin, but they needed to identify who. Could a court authorize a warrant for police to search everyone in the bar to figure out who was the possessor? No. No court would properly authorize such a warrant.”).

247. *See id.*

248. *See Ybarra*, 444 U.S. at 91 (articulating the principle that mere propinquity is insufficient for probable cause); *see also Maryland v. Pringle*, 540 U.S. 366, 371 (2003) (reaffirming probable cause “must be particularized with respect to the person to be searched or seized”); *Groh v. Ramirez*, 540 U.S. 551, 563 (2004) (explaining that the objective standard for good-faith exception requires officers to have reasonable knowledge of what the law prohibits); *United States v. Chatrie*, 136 F.4th 100, 160 (4th Cir. 2025) (Gregory, J., dissenting) (noting an officer is presumed to know that information in warrant was insufficient because “it was not unclear what the Constitution demands of all warrants[]”).

249. *See Ybarra*, 444 U.S. at 91; *Pringle*, 540 U.S. at 371; *Groh*, 540 U.S. at 563; *Chatrie*, 135 F.4th at 157 (Gregory, J., dissenting).

250. *See United States v. Chatrie*, 590 F. Supp. 3d 901, 932–33 (E.D. Va. 2022), *aff’d en banc*, 107 F.4th 319 (4th Cir. 2024), *aff’d on reh’g*, 136 F.4th 100 (4th Cir. 2025), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026); *United States v. Fuentes*, No. CR-21-358-RAW, 2024 WL 5494054, at *5–6 (E.D. Okla. Sep. 3, 2024); *State v. Baldwin*, 664 S.W.3d 122, 135 (Tex. Crim. App. 2022) (affirming the “trial court’s conclusion that the affidavit contained insufficient particularized facts” to establish probable cause to search a cell phone).

Courts have long criticized warrant applications that are so conclusory and devoid of facts that no reasonable officer could rely on them.²⁵¹ The Supreme Court in *Illinois v. Gates* made this clear: probable cause needs concrete facts, not speculative generalizations.²⁵² Nevertheless, the affidavits for geofences frequently present rehashed statistics on the use of smartphones in modern times, the generic description of Google's Sensorvault, the indefinite assertion that criminals use location-enabled devices, and template language about location history.²⁵³ None of this is case-specific. Instead, it is copied from previous applications or "ghostwritten" by prosecutors to sound technologically advanced without giving any real support to probable cause.²⁵⁴ These affidavits are nothing more than "a mere ratification of the bare conclusions of others," precisely what *Gates* prohibits.²⁵⁵

The Fourth Amendment requires that, to constitute probable cause, there should be a factual nexus between the alleged criminal activity and the particular person, place, or thing to be searched or seized.²⁵⁶ Geofence warrants are the opposite. They draw a digital circle around a crime scene and force Google to surrender location data for every device entering that space, without any prior identification of suspects.²⁵⁷ That is not a nexus. It's a net. Attaching suspicion to a place instead of a person turns the Fourth Amendment upside down.²⁵⁸ No reasonable officer could believe that such a broad, untargeted search satisfies probable cause because it attaches suspicion to places rather than people.²⁵⁹

251. See *Illinois v. Gates*, 462 U.S. 213, 239 (1983).

252. See *id.* (explaining a magistrate "cannot [simply ratify] the bare conclusions of others" and conclusory allegations alone are insufficient); *Baldwin*, 664 S.W.3d at 134 ("[B]oilerplate language about cell phone use among criminals [is not] sufficient to establish probable cause to search a cell phone[.]").

253. See *Baldwin*, 664 S.W.3d at 134; see also *In re Search of Info. Stored at Premises Controlled by Google*, No. 20 M 297, 2020 WL 5491763, at *3 n.3 (N.D. Ill. July 8, 2020) (showing the government asserted the ubiquity of Google products and that nearly all smartphones use Google apps, making it likely any given phone is interfacing with Google).

254. See *Fuentes*, 2024 WL 5494054, at *6 (documenting when the affiant, Thornton, testified that probable cause sections were "authored by Assistant United States Attorney James Montoya[]"); see also *United States v. Smith*, 110 F.4th 817, 826 ("[Postal] Inspectors used several different 'go-bys'—or form documents—to ensure that their application had all the necessary 'technical language.'").

255. *Gates*, 462 U.S. at 239 (warning against magistrates "mere[ly] ratify[ing] the bare conclusions of others").

256. See U.S. CONST. amend. IV; *In re Search of Info. Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d 62, 75 (D.D.C. 2021) (citing *United States v. Griffith*, 867 F.3d 1265, 1271 (D.C. Cir. 2017)).

257. See *United States v. Rhine*, 652 F. Supp. 3d 38, 66 (D.D.C. 2023) (explaining geofencing is a technique law enforcement "utilize[s] when the crime location is known but the identities of suspects [are] not[]"); see also Google Amicus Brief, *supra* note 4, at 3 (describing geofence requests as having no particularized basis, just where users were at a given time).

258. See *Smith*, 110 F.4th at 837 (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)) ("Geofence warrants present the exact sort of 'general, exploratory rummaging' that the Fourth Amendment was designed to prevent.").

259. See *United States v. Chatrue*, 136 F.4th 100, 160 (4th Cir. 2025) (Gregory, J., dissenting) (explaining "an officer need not know the [J]udiciary's view on the use of new technology" to know that "it was not unclear what the Constitution demands of all warrants[]"); *In re Search of Info. Stored at*

In *State v. Baldwin*, the Texas Court of Criminal Appeals held that generic language about cell phone use by criminals does not create enough probable cause to search a device.²⁶⁰ Similarly, in the case of geofence warrants, phrases like “the perpetrator might have used a phone” or “Google may have location data” are also very unlikely.²⁶¹ In *Chatrie*, Justice Wynn’s dissent emphasized this point, arguing that boilerplate reducing probable cause to “the robber used a cell phone and a cell phone *could* have Google Location History turned on [] is extremely broad” and fails to justify the intrusion.²⁶² That’s barely an idea, let alone probable cause.

The use of standard templates and ghostwritten content is a sign of the significant problem with the geofence process.²⁶³ In *United States v. Fuentes*, officers investigating a hit-and-run applied for a geofence warrant without identifying any suspect, device, or connection between any phone and the crime.²⁶⁴ The affidavit was littered with studies on cell phones being common in vehicles, and the court found it was ghostwritten by someone else.²⁶⁵ When an affidavit’s source of content is so unclear and the facts are so thin, no reasonable officer could view it as supporting probable cause.²⁶⁶ The court concluded that reliance on such an affidavit “falls short of good faith and mandates the suppression of the evidence derived from the Google search.”²⁶⁷

The three-step geofence process does not fix any of this. As explained above, probable cause must exist at the time of issuance, not after investigators dig through data.²⁶⁸ However, geofences usually involve an initial indiscriminate sweep of all devices in the area, followed by

Premises Controlled by Google, No. KM-2022-79, 2022 WL 584326, at *9 (Va. Cir. Ct. Feb. 24, 2022) (noting that no court would properly authorize a warrant “to search everyone in the bar to figure out who was the possessor[]” in the *Ybarra* scenario).

260. See *State v. Baldwin*, 664 S.W.3d 122, 134 (Tex. Crim. App. 2022) (“[S]pecific facts connecting the items to be searched to the alleged offense are required To hold otherwise would condone the search of a phone merely because a person is suspected to have committed a crime with another person.”).

261. See *United States v. Chatrie*, 107 F.4th 319, 362 n.12 (4th Cir. 2024) (Wynn, J., dissenting), *aff’d on reh’g*, 136 F.4th 100 (4th Cir. 2025), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026).

262. *Id.*

263. See *Smith*, 110 F.4th at 826.

264. See *United States v. Fuentes*, No. CR-21-358-RAW, 2024 WL 5494054, at *11 (E.D. Okla. Sep. 3, 2024) (noting that the affidavit was “completely lacking any facts to indicate that the perpetrator of the offense possessed a cell phone” or that phone was connected to Google’s Location History).

265. *Id.* at *5 (“Paragraphs 24 and 25 in the [a]ffidavit reference studies on the prevalence of cell phones in motor vehicles.”).

266. *Id.* at *11 (noting an affiant’s attestation that information was “‘based upon his training and experience’ was simply false” given ghostwriting); see also *United States v. Leon*, 468 U.S. 897, 923 (1984) (quoting *Brown v. Illinois*, 422 U.S. 590, 610–11 (1975) (Powell, J., concurring)) (holding the good-faith exception does not apply when an affidavit is “so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable[]” (internal quotations omitted)).

267. *Fuentes*, 2024 WL 5494054, at *11.

268. See *Smith v. Munday*, 848 F.3d 248, 253 (4th Cir. 2017).

law-enforcement-led narrowing after the fact.²⁶⁹ Officers cannot know which devices are relevant up front, so probable cause is absent for nearly all searched accounts.²⁷⁰ Judicial review is skipped, and the warrant becomes a general exploratory tool.²⁷¹ Hoping that later narrowing will justify the first intrusion contradicts everything the Fourth Amendment demands.²⁷²

No reasonable officer could believe this complies with the Constitution.²⁷³ The warrant clause requires that a judge, not an officer, not a private entity, determine probable cause before the search.²⁷⁴ Geofence warrant searches ignore this requirement.²⁷⁵

Even if an officer could somehow believe that proximity creates probable cause, the overbreadth of these warrants renders any argument for their validity moot.²⁷⁶ Geofence warrants inevitably capture data from numerous uninvolved individuals who have no connection to the crime beyond geographic proximity.²⁷⁷

As documented above, the ACLU's analysis of San Francisco geofence warrants revealed systematic sweeps of homes, apartment buildings, workplaces, places of worship, medical facilities, and schools.²⁷⁸ This was

269. See *United States v. Smith*, 110 F.4th 817, 836–37 (5th Cir. 2024) (explaining that geofence warrants are “general warrants” because the search is “occurring while law enforcement officials have *no idea* who they are looking for”).

270. See *Pharma II*, 481 F. Supp. 3d 730, 753 (N.D. Ill. 2020) (noting a warrant that captured devices “based on nothing other than their close proximity,” violated the requirement for probable cause).

271. *Id.*

272. *Id.*

273. See *Groh v. Ramirez*, 540 U.S. 551, 563 (2004) (holding “no reasonable officer could believe that a warrant that plainly did not comply with [the particularity] requirement was valid”); see also *United States v. Chatrie*, 136 F.4th 100, 159 (4th Cir. 2025) (Gregory, J., dissenting) (stating no reasonable officer could believe that the execution of geofence warrants in this manner comports with Fourth Amendment, which “explicitly demands” specificity).

274. See U.S. CONST. amend. IV; *Johnson v. United States*, 333 U.S. 10, 14 (1948) (explaining that the probable cause decision is “to be decided by a judicial officer, not by a policeman or [g]overnment enforcement agent”).

275. See *Chatrie*, 136 F.4th at 159 (Gregory, J., dissenting) (noting that the warrant “ceded authority and decision-making from an independent judicial officer to a private corporation”); see also *United States v. Smith*, 110 F.4th 817, 838 n.12 (5th Cir. 2024) (“Google’s actions, including at Step 1, are ‘conducted in response to legal compulsion’” and Google acts as “an instrument or agent of the Government”).

276. See *United States v. Chatrie*, 590 F. Supp. 3d 901, 929 (E.D. Va. 2022), *aff’d en banc*, 107 F.4th 319 (4th Cir. 2024), *aff’d on reh’g*, 136 F.4th 100 (4th Cir. 2025), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026) (finding the warrant was overbroad because it was “completely devoid of any suggestion that all—or even a substantial number of—the individuals searched had participated in or witnessed the crime”); *In re Search of Info. Stored at Premises Controlled by Google, as Further Described in Attachment A*, No. 20-M-297, 2020 WL 5491763, at *5 (N.D. Ill. July 8, 2020) (ruling that geofence location was overbroad because the vast majority of cellular telephones likely to be identified in it “[would] have nothing whatsoever to do with the offenses under investigation”).

277. See *People v. Meza*, 312 Cal. Rptr. 3d 1, 18 (Cal. Ct. App. 2023) (“The failure to sufficiently narrow the search parameters potentially allowed a location-specific identification of thousands of individuals . . . for whom no probable cause existed.”); *Smith*, 110 F.4th at 826 (noting that false positives—devices belonging to innocent individuals—“are still an area of concern”).

278. See Snow, *supra* note 150 (analyzing San Francisco geofence warrants and finding that geofences covered hundreds of residences, twelve places of worship, seven medical sites of care, and other private spaces).

not accidental; instead, it was an inevitable result of geofence methodology.²⁷⁹ When a warrant allows an officer to draw a 300-meter radius in a populated area, it will capture innocent people.²⁸⁰ Without any factual or probable basis to believe that evidence will be found on any particular device among the hundreds or thousands of devices captured, probable cause collapses.²⁸¹ An officer reviewing such an application should see immediately that the application assigns suspicion to a crowd, not a person.

These warrants force officers into guesswork, and applicants fill evidentiary holes with assumptions.²⁸² This systemic guesswork poisons the warrant process and prioritizes convenience over constitutional safeguards. No reasonable officer, bound by training and precedent, could deem this reasonable.²⁸³ Affidavits justify a geofence search based on the assumption that if a perpetrator had an Android device, Google might possess identifying information.²⁸⁴ These searches often return data from devices that are not linked to any suspect, highlighting the absence of probable cause for any particular account.²⁸⁵ Officers cannot know in advance which devices are relevant, and the initial affidavit that the government submits to the magistrate judge provides no individualized evidence for the included devices.²⁸⁶

Therefore, geofence warrants do not suffer from weak probable cause; they lack it entirely.²⁸⁷ The fact that they are grounded on mere speculation, copy-and-paste affidavits, their overly broad nature, and the procedural shortcuts make good-faith reliance under *Leon* impossible.²⁸⁸ This isn't a new

279. *See id.*

280. *See Chatrie*, 590 F. Supp. 3d at 918 (noting that the warrant covered an area the size of three football fields, with a confidence interval reach even larger); *see also Meza*, 312 Cal. Rptr. 3d at 6 (finding that a geofence can be “any size or shape”).

281. *See In re Search of Info. That is Stored at the Premises Controlled by Google, LLC*, 542 F. Supp. 3d 1153, 1157 (D. Kan. 2021).

282. *See Smith*, 110 F.4th at 837 (finding that warrants are susceptible to being used as “general, exploratory rummaging” that the Fourth Amendment prohibits); *United States v. Fuentes*, No. CR-21-358-RAW, 2024 WL 5494054, at *11 (E.D. Okla. Sep. 3, 2024) (noting that the affiant admitted “he had actual knowledge of very little of the information provided” in the affidavit, highlighting the reliance on external input and lack of officer knowledge).

283. *See United States v. Chatrie*, 136 F.4th 100, 157, 159 (4th Cir. 2025) (Gregory, J., dissenting) (“No reasonable officer could believe that execution of this geofence warrant in this manner comports with the Fourth Amendment . . .”).

284. *See Chatrie*, 590 F. Supp. 3d at 932–33.

285. *See O'Connor*, *supra* note 41.

286. *See Chatrie*, 136 F.4th at 155 (Berner, J., concurring) (noting that “the detective could not explain why he would eventually search the Location History data of certain, then-unknown users” and “he failed to show probable cause to conduct the second and third requests”).

287. *See id.* at 153 (Berner, J., concurring) (finding that the information provided to the magistrate—users would be among those near the crime scene—“unequivocally falls short of establishing probable cause”).

288. *See United States v. Leon*, 468 U.S. 897, 923 (1984) (quoting *Brown v. Illinois*, 422 U.S. 590, 610–11 (1975)) (stating that the good-faith exception does not apply when an affidavit is “so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable”) (internal quotations omitted); *Chatrie*, 136 F.4th at 159 (Gregory, J., dissenting) (arguing that the good-faith

issue. It echoes long-standing prohibitions of broad searches without any suspicion of a particular individual.²⁸⁹ Suppression is not optional; it is required.

C. When Particularity Becomes a Guessing Game: Warrants So Facially Deficient that Officers Cannot Presume Them Valid

The fourth circumstance under which the *Leon* good-faith exception does not apply is when the warrant is “so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid.”²⁹⁰ This exception serves as the Fourth Amendment’s explicit requirement that warrants must “particularly describ[e] the place to be searched, and the persons or things to be seized.”²⁹¹

Geofence warrants fail the particularity requirement firstly by allowing indiscriminate and sweeping searches, and secondly, by giving officers unbridled discretion over the next steps.²⁹² This shortcoming is so glaringly evident from the face of the warrant that no reasonable officer could presume it to be valid under *Leon*.²⁹³ In contrast to a situation where the ambiguous language of the warrant may confuse an executing officer, in the case of geofence warrants, there are facial violations which any officer examining the four corners of the warrant would immediately recognize as constitutionally deficient.²⁹⁴

exception should not apply because the officer failed to seek judicial intervention and the warrant lacked sufficient probable cause and particularity, granting “unbridled discretion”).

289. See *Carpenter v. United States*, 585 U.S. 296, 316 (2018) (holding that the Fourth Amendment protects an individual’s expectation of privacy in the recording of their physical movements and generally requires a warrant supported by probable cause and particularity); *Ybarra v. Illinois*, 444 U.S. 85, 86, 90 (1979) (requiring probable cause to be particularized with respect to the person to be searched or seized and noting “mere propinquity to others” is insufficient).

290. *Leon*, 468 U.S. at 923.

291. U.S. CONST. amend. IV.

292. See *supra* Section III.C (explaining how geofence warrants fail the particularity requirement).

293. See *Leon*, 468 U.S. at 923 (suppression is mandatory if the warrant is “so facially deficient” that officers cannot “reasonably presume it to be valid”); *Chatrle*, 136 F.4th at 157 (Gregory, J., dissenting) (explaining that the warrant was facially deficient and lacked requisite constitutional requirements, leading to the conclusion that “[n]o reasonable officer could believe that execution of this geofence warrant in this manner comports with the Fourth Amendment”).

294. See *Chatrle*, 136 F.4th at 160 (Gregory, J., dissenting) (arguing “an officer need not know the judiciary’s view on . . . new technology . . . to know that the information in the warrant was insufficient” as “it was not unclear what the Constitution demands of all warrants[]”); *United States v. Smith*, 110 F.4th 817, 837–38 (5th Cir. 2024) (emphasizing deficiency is inherent in design: Geofence warrants are “categorically prohibited” general warrants because they initiate a search where law enforcement “have no idea who they are looking for”).

1. Fourth Amendment Commands Are Unambiguous

The particularity requirement is not a subtle doctrine hidden in case law.²⁹⁵ It is explicit.²⁹⁶ When a warrant fails to particularly describe the persons or things to be searched, the defect isn't a matter of constitutional interpretation.²⁹⁷ It is a direct violation of the Amendment's text.²⁹⁸ Officers must have "reasonable knowledge of what the law prohibits,"²⁹⁹ and the Fourth Amendment's requirement for particularity and probable cause has been settled since the Founding.³⁰⁰ A claim of confusion cannot save a warrant that broadcasts its invalidity on its face.³⁰¹

When a warrant facially fails to describe the persons or things to be searched, the deficiency is not a legal question surrounded by legal undertones; it is a violation of the Amendment's plain language.³⁰²

2. Geofence Warrants Not Only Dodge Particularity, They Flip It Upside Down

These warrants do more than fail the particularity requirement; they invert it entirely. By handing officers a blank check to rummage through digital lives without limits or objective criteria, geofence warrants resemble the same general warrants the Founders warned about.³⁰³ Geofence warrants' defects are glaring and render good-faith reliance not only unsustainable but constitutionally offensive.

295. See U.S. CONST. amend. IV.

296. *Id.*

297. *Id.*

298. See *id.*; *Marron v. United States*, 275 U.S. 192, 196 (1927) (particularity requirement "makes general searches under them impossible" and ensures "nothing is left to the discretion of the officer executing the warrant").

299. *United States v. Leon*, 468 U.S. 897, 919 n.20 (1984) (citing *United States v. Peltier*, 422 U.S. 531, 542 (1975)); see also *Groh v. Ramirez*, 540 U.S. 551, 563; *Chatrle*, 136 F.4th at 157 (Gregory, J., dissenting) (noting changes in technology do not affect constitutional warrant requirements).

300. See *Steagald v. United States*, 451 U.S. 204, 220 (1981) (clarifying the Fourth Amendment was in response to the reviled "general warrants" and "writs of assistance" of the Colonial Era).

301. See *Chatrle*, 136 F.4th at 160 (Gregory, J., dissenting) (endorsing forgiving impropriety because no court has specifically forbidden it, as it "would run the risk of forgiving law enforcement impropriety simply because no court has specifically forbidden it," rendering Fourth Amendment protections "a nullity in the face of rapidly emerging technology"); *Leon*, 468 U.S. at 912 n.9 (cautioning against "a let's-wait-until-it's-decided approach" to constitutional violations).

302. See U.S. CONST. amend. IV.

303. *In re Search of Info. Stored at Premises Controlled by Google*, No. KM-2022-79, 2022 WL 584326, at *9 (Va. Cir. Ct. Feb. 24, 2022) (identifying the geofence warrant application as a proverbial blank check); see also *United States v. Smith*, 110 F.4th 817, 837 (5th Cir. 2024) (holding geofence warrants are general warrants categorically prohibited by the Fourth Amendment because law enforcement "have no idea who they are looking for"); *Chatrle*, 136 F.4th at 157 (Gregory, J., dissenting) (holding the warrant granted unbridled discretion that lacked the specificity the Fourth Amendment demands).

The particularity clause, which is one of the requirements that can be traced back to the Founding, requires that warrants indicate their extent with exactness so that there would be no discretion left to the officers who are executing it.³⁰⁴ A warrant specifying only an offense, without explaining the decision-making process as to whom or what to search, is per se invalid.³⁰⁵ Yet geofence warrants systematically ignore this requirement, giving officers complete discretion over the search's evolution.³⁰⁶ Providing no objective guardrails, these warrants authorize an initial sweep of anonymized device data from an at times inexplicable virtual perimeter, then empower investigators to expand, refine, and unmask at will, without defined standards or renewed judicial scrutiny.³⁰⁷ This structure transforms the warrant into an open license for exploratory surveillance that the Fourth Amendment was crafted to abolish.³⁰⁸

3. Google's Three-Step Process Invites, Rather Than Controls, Discretion

The three-step process that geofences use renders the warrants facially deficient and prevents any reasonable presumption of validity.³⁰⁹ Steps Two and Three turn into officer-led free-for-alls with investigators unilaterally filtering the list by subjective judgments,³¹⁰ requesting extended tracking beyond the original boundaries,³¹¹ and demanding identifying information for selected accounts.³¹²

304. See *Steagald*, 451 U.S. at 220 (noting that a general warrant specifies “only an offense . . . and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched”).

305. *Id.*

306. See *People v. Meza*, 312 Cal. Rptr. 3d 1, 23–24 (Cal. Ct. App. 2023) (holding the warrant was insufficiently particular “because it provided law enforcement with unbridled discretion regarding whether or how to narrow the initial list of users”); *Pharma II*, 481 F. Supp. 3d 730, 754 (N.D. Ill. 2020) (denying geofence warrant application because “the warrant puts no limit on the government’s discretion to select the device IDs” for identifying information).

307. See *supra* Sections II.B, III.C (discussing Google’s three-step process for geofence warrants and its broad, untailored scope).

308. See *Smith*, 110 F.4th at 837 (“Geofence warrants present the exact sort of ‘general, exploratory rummaging’ that the Fourth Amendment was designed to prevent.”); *United States v. Fuentes*, No. CR-21-358-RAW, 2024 WL 5494054, at *5 (E.D. Okla. Sep. 3, 2024) (describing the “hallmark of a general warrant—aimless searching with only the hope that the result will justify the means”).

309. See *United States v. Chatrie*, 136 F.4th 100, 137 (4th Cir. 2025) (Gregory, J., dissenting) (where the warrant was “so facially deficient” that no reasonable officer could believe its execution comports with the Fourth Amendment); *Meza*, 312 Cal. Rptr. 3d at 23–24.

310. See *In re Search of Info. Stored at Premises Controlled by Google*, No. KM-2022-79, 2022 WL 584326, at *9 (Va. Cir. Ct. Feb. 24, 2022).

311. See *United States v. Chatrie*, 590 F. Supp. 3d 901, 916 (E.D. Va. 2022), *aff’d en banc*, 107 F.4th 319 (4th Cir. 2024), *aff’d on reh’g*, 136 F.4th 100 (4th Cir. 2025), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026) (Step Two allows law enforcement to obtain “additional location data outside the original request’s scope”).

312. See *Meza*, 312 Cal. Rptr. 3d at 24 (indicating at Step Three, “law enforcement could seek identifying information . . . without restriction . . . or any further showing that information concerning each individual user would be relevant”).

As the *Meza* court observed, such warrants “fail[] to meet the particularity requirement because [they] provide[] law enforcement with unbridled discretion regarding whether or how to narrow the initial list of users identified by Google.”³¹³ Post-Step One, officers can “enlarge the geographic parameters of the search and request additional information on any of the potentially thousands of users identified without any objective criteria limiting their discretion.”³¹⁴ At Step Three, this escalates further: law enforcement may “seek identifying information of any of the users found within the search parameters without restriction on how many users could be identified or any further showing that information concerning each user would be relevant to the case.”³¹⁵ This is not a narrowing process; it is an invitation to abuse, where officers, not judges, dictate the search’s depth and breadth.

Courts have called this model out for what it ultimately is—an unconstitutional blank check.³¹⁶ A Virginia court in *In re Search of Information Stored at Premises Controlled by Google*, rejected a geofence application, singling out the proposal’s Step Two as the point where the officer can “unilaterally: (1) determine cell phone relevancy, and (2) enlarge the [c]ourt-authorized search zone.”³¹⁷ The court found that the application was clearly overbroad, and it gave officers the power to change the geofence boundaries mid-execution, thus allowing devices to be potentially caught without any justification or control.³¹⁸ Equally, the Fifth Circuit in *United States v. Smith* referred to geofence warrants as “modern-day general warrants.”³¹⁹

This issue is widespread; for instance, in *Chatrie*, the terms of the warrant gave the law enforcement officer the authority to enact a sweeping search.³²⁰ The geofence spanned a 300-meter space in a downtown area—equivalent to three football fields—with an even larger confidence interval, yielding nineteen anonymized device IDs in Step One.³²¹ At Step Two, the law enforcement officer arbitrarily narrowed the list down to nine devices, demanding their movements outside the geofence for an hour pre and post-robbery “without any geographic limitations,” and without providing

313. *Id.* at 538.

314. *Id.*

315. *Id.*

316. *In re Search of Info. Stored at Premises Controlled by Google*, No. KM-2022-79, 2022 WL 584326, at *9 (Va. Cir. Ct. Feb. 24, 2022).

317. *Id.*

318. *Id.*

319. *United States v. Smith*, 110 F.4th 817, 840 (5th Cir. 2024).

320. *See United States v. Chatrie*, 590 F. Supp. 3d 901, 934 (E.D. Va. 2022), *aff’d en banc*, 107 F.4th 319 (4th Cir. 2024), *aff’d on reh’g*, 136 F.4th 100 (4th Cir. 2025), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026) (finding warrant Steps Two and Three “improperly provided law enforcement and Google with unbridled discretion to decide which accounts will be subject to further intrusions”).

321. *See Chatrie*, 136 F.4th at 104–05 (Diaz, C.J., concurring).

objective criteria or judicial approval.³²² The officer never clarified why or how these nine devices, out of the rest, were connected to the crime apart from their presence at the scene.³²³

The actions of the law enforcement officer at Step Three only escalated the constitutional breach. Law enforcement requested Google, not a magistrate judge, to reveal all nine devices.³²⁴ When Google refused that request, officers then chose three accounts to unmask without any probable cause and did not tell Google why those devices were chosen.³²⁵ As the certiorari petition suitably frames it:

Detective Hylton . . . conducted a warrantless search without probable cause. [He] lacked probable cause to investigate those three accounts: he offered no reasoning to Google as to why these three accounts were singled out. And even if Detective Hylton offered such reasoning, Google is not a magistrate judge.³²⁶

This sequence is one of many cases that reveal the same core defect.³²⁷ A geofence warrant authorizes increasingly intrusive searches without essential constitutional limitation, leaving officers to wield power the Fourth Amendment reserves for neutral judges.³²⁸

This is the exact unrestrained discretion seen in the Supreme Court's decision not to extend *Leon*'s good-faith exception in *Groh v. Ramirez*.³²⁹ In that case, the local authorities conducted a warrantless search because the warrant did not describe the items to be seized.³³⁰ Hence, it was "so obviously deficient" that the Court refrained from considering it a valid search.³³¹ The Court recognized that no reasonable officer could rely on such an apparent void as it violates the Fourth Amendment's explicit particularity requirement.³³²

Geofence warrants are guilty of a comparable offense: they do not particularly describe either persons or things, but they allow officers to make

322. *Id.* at 159 (Gregory, J., dissenting).

323. *See id.* at 126 (Wynn, J., concurring).

324. *See id.* at 133 (Richardson, J., concurring).

325. *Id.*

326. Chatrie Pet. for Cert., *supra* note 31, at 33.

327. *See Chatrie*, 136 F.4th at 137 (Gregory, J., dissenting) (noting that the "warrant lacked the requisite constitutional requirements to conduct increasingly intrusive searches at Steps Two and Three" and "ceded authority and decision-making from an independent judicial officer to a private corporation"; *see also* *United States v. Smith*, 110 F.4th 817, 837 (5th Cir 2024) ("Geofence warrants present the exact sort of 'general, exploratory rummaging' that Fourth Amendment was designed to prevent.")).

328. *See, e.g., Chatrie*, 136 F.4th at 137 (Gregory, J., dissenting) (indicating warrant lacked constitutional requirements but granted anyways); *see also Smith*, 110 F.4th at 837 (finding geofence warrants required exploratory rummaging, which the Fourth Amendment was designed to prevent).

329. *See Groh v. Ramirez*, 540 U.S. 551, 563–64 (2004).

330. *Id.*

331. *Id.* at 557.

332. *Id.*

those decisions.³³³ Unlike cases of ambiguity where officers might plausibly misinterpret scope, geofence flaws are structural and self-evident.³³⁴

Under *Leon*, officers are required to have “reasonable knowledge of what the law prohibits.”³³⁵ The Fourth Amendment’s textual ban of general warrants is a fundamental principle supported by precedent dating back to the Founding.³³⁶ Reasonable officers cannot claim ignorance if a warrant grants officers unlimited decision-making power.³³⁷ To find good-faith reliance in these warrants would encourage affidavits that deliberately undermine the magistrate’s gatekeeping role and embody the very abuse the Particularity Clause targets.³³⁸ In this case, suppression is necessary, not as punishment, but as the Constitution’s remedy for warrants that no officer could reasonably consider valid.³³⁹

Therefore, geofence searches fall squarely under *Leon*’s exceptions due to magistrate abandonment, deficient affidavits, facially invalid warrants, and flaws left unaddressed.³⁴⁰ This enhances the *Leon* loophole that only legislation can close.

V. LEGISLATION IS THE ANSWER: THE GEOFENCE LOCATION DATA ACCESS ACT

Building on the analysis above, the Geofence Location Data Access Act emerges as the necessary remedy. It is undeniable that geofence warrants present serious Fourth Amendment concerns.³⁴¹ Their increased use and the lack of critical statutory or judicial guidelines leave geofence warrants unbound, enabling law enforcement to intrude into the private lives of many.³⁴² However, instead of confronting these issues, courts refuse to make necessary constitutional decisions and hide behind the good-faith standard in

333. See, e.g., *United States v. Smith*, 110 F.4th 817, 837–38 (5th Cir. 2024) (lacking particularity necessary for a Fourth Amendment search).

334. See *People v. Meza*, 312 Cal. Rptr. 3d 1, 16 (Cal. Ct. App. 2023) (noting no ambiguity in database or initial targets but invalidity stemmed from post-issuance discretion).

335. *United States v. Leon*, 468 U.S. 897, 919 n.20 (1984) (quoting *United States v. Peltier*, 422 U.S. 531, 542 (1975)).

336. See U.S. CONST. amend. IV; *Steagald v. United States*, 451 U.S. 204, 220 (1981).

337. See *Chatrue*, 136 F.4th at 159 (Gregory, J., dissenting) (“[T]he warrant ceded authority and decision-making from an independent judicial officer to a private corporation. No reasonable officer could believe that . . . comports with the Fourth Amendment.”).

338. See *id.* at 160 (endorsing the practice of forgiving impropriety due to a lack of precedent would “run the risk of forgiving law enforcement impropriety simply because no court has specifically forbidden it”).

339. See *id.* at 160 (concluding that “[e]xclusion of the evidence [was] . . . appropriate” because warrant gave decision-making authority to private corporation and lacked constitutional requirements).

340. See *supra* notes 195–204 and accompanying text (explaining how the overbroad nature of geofence warrants result in abdication of judicial oversight).

341. See *supra* Part III (explaining why geofence warrants violate the Fourth Amendment).

342. See Google Amicus Brief, *supra* note 4, at 3 (noting an 1,500% increase in geofence requests from law enforcement).

Leon.³⁴³ While it is true that states have proactively passed legislation on geofence warrants, they are just as divided as the courts.³⁴⁴ The result is a national patchwork that provides no clarity to law enforcement nor meaningful protections to the public. Congress must act.

This will not be the first time Congress has stepped in to regulate an investigative tool when courts and states could not find a uniform approach.³⁴⁵ In 1968, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III) in response to widespread, unregulated wiretapping.³⁴⁶ It specifically passed Title III in response to congressional investigations and published studies that found government agencies and private individuals had conducted “extensive wiretapping” without the consent of the parties or legal sanction.³⁴⁷ Title III imposed heightened warrant requirements—and to use a wiretap, law enforcement must provide more information in the warrant application.³⁴⁸ Specifically, these warrants were allowed only to investigate certain crimes, and law enforcement had to explain whether it used other investigative measures or why other techniques were likely to fail or were too dangerous.³⁴⁹ Additionally, law enforcement must monitor the wiretap and ensure that conversations unrelated to the underlying offense were not intercepted.³⁵⁰

Geofence warrants present the same structural issue that wiretaps did. They are powerful, invasive tools being used without any statute to guide them.³⁵¹ Until there is a uniform approach to these, their use and subsequent constitutional issues will remain unanswered until Congress provides clear rules. Therefore, this Comment proposes federal legislation modeled after Title III to regulate geofence warrants. This legislation would finally bring order to this widespread chaos, laying out clear and consistent procedures and providing real constitutional limits.³⁵² Ultimately, these powerful tools must be used only when necessary and in a way that respects the Fourth Amendment, rather than leaving everything to guesswork and good faith. On

343. See *United States v. Chatrie*, 136 F.4th 100, 115 (Wynn, J. concurring) (admonishing the court for declining to reach the merits on the case, and instead using good faith as a shield).

344. See, e.g., N.Y. GEN. BUS. LAW § 394-g (McKinney 2023) (banning geofencing around health care facilities, except their own virtual boundary of 1,850 feet); CONN. GEN. STAT. § 42-520 (2023) (Connecticut’s Data Privacy Act prohibits use of geofence “to establish a virtual boundary that is within [1,750] feet of any mental health facility or reproductive or sexual health facility for the purpose of identifying, tracking, collecting data from or sending any notification to a consumer regarding the consumer’s consumer health data”); WASH. REV. CODE § 19.373.005–.900 (2023) (Washington My Health My Data Act); NEV. REV. STAT. § 603A.010–.920 (2021) (Nevada’s data breach statute).

345. See Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 802, 82 Stat. 197, 211 (1968) (codified as amended at 18 U.S.C. §§ 2510–2522).

346. *Id.*

347. S. REP. NO. 90-1097, at 2177 (1968).

348. See Omnibus Crime Control and Safe Streets Act § 802.

349. *Id.*

350. *Id.*

351. See GEOFENCE WARRANT PRIMER, *supra* note 4, at 1–2.

352. See *infra* Appendix (proposing legislation).

June 29, 2026, the Supreme Court decided *Chatrie v. United States*, resolving by a 6–3 vote the very question Section III.A of this Comment treats as a threshold matter: whether accessing Location History through a geofence warrant is a Fourth Amendment search at all.³⁵³ Writing for five Justices, Justice Kagan extended *Carpenter v. United States* to Google’s Location History service, holding the data even more revealing than the cell-site records at issue in *Carpenter*, capable of the same “retrospective” and tireless surveillance *Carpenter* condemned, and not “truly shared” with Google merely because a user enabled the feature to make his phone work as intended.³⁵⁴ The Court also rejected the Government’s argument that the mere 2-hour duration of the data sought placed it outside the Fourth Amendment altogether, reaffirming that the Amendment applies no matter how much or what kind of information the government obtains.³⁵⁵ Justice Gorsuch supplied the sixth vote for the same result through an entirely different, property-based theory of Chatrie’s data as an “effect,” while Justices Alito, Thomas, and Barrett dissented on the theory that the third-party doctrine controls.³⁵⁶ The Supreme Court’s decision thus nationalizes the search question and supports the position this Comment takes in Section III.A, as well as partially resolving the circuit split described in Section II.D.³⁵⁷

The Supreme Court’s decision, however, resolves only the threshold question; it leaves untouched the problems Sections III.B, III.C, and Part IV identifies as the real defect in geofence practice.³⁵⁸ The Court expressly declined to decide “whether, at each step of the search process, the warrant satisfied the Fourth Amendment’s requirements of particularity and probable cause,” remanding that inquiry to the Fourth Circuit as “a court of review, not of first view.”³⁵⁹ Eight years after *Carpenter*, and now after *Chatrie*, the

353. *Chatrie v. United States*, No. 25-112, 2026 WL 1855568, at *4 (U.S. June 29, 2026); *see also supra* Section III.A (explaining why Location History implicates a reasonable expectation of privacy).

354. *Chatrie*, No. 25-112, 2026 WL 1855568, at *15 (citing *Carpenter v. United States*, 585 U.S. 296, 315 (2018)) (extending *Carpenter v. United States* to Location History and concluding that a user does not meaningfully share that data with Google in the sense the third-party doctrine requires).

355. *Id.* at *13 (quoting *Kyllo v. United States*, 533 U.S. 27, 37 (2001)).

356. *Id.* at *19–22 (Gorsuch, J., concurring); *id.* at *22–30 (Alito, J., dissenting); *id.* at *30 (Barrett, J., dissenting).

357. *See supra* Section III.A (arguing that accessing Location History through a geofence warrant is a Fourth Amendment search because the data is at least as revealing as the CSLI at issue in *Carpenter* and is not meaningfully shared with Google in the sense the third-party doctrine requires); *see also supra* Section II.D (cataloging the split among state and federal courts over whether accessing Location History through a geofence warrant is a Fourth Amendment search, including the Fourth Circuit’s own en banc decision below, which divided evenly on that very question).

358. *Contrast Chatrie*, No. 25-112, 2026 WL 1855568 at *4 (only deciding whether accessing Location History is a Fourth Amendment search), with *supra* Section III.B (discussing the lack of probable cause in geofence warrants), and *supra* Section III.C (explaining how geofence warrants fail the particularity requirement), and *supra* Part IV (arguing why Leon’s good-faith exception does not apply to geofence warrants).

359. *Chatrie*, No. 25-112, 2026 WL 1855568 at *17 (quoting *Cutter v. Wilkinson*, 544 U.S. 709, 718 n.7 (2005)).

Supreme Court still has not said how large a geofence may be, what showing must justify Step Two's expansion beyond the original perimeter, or what criteria—if any—must appear on a warrant's face before officers may unmask a Step Three subset of users.³⁶⁰ Only Justice Jackson's concurrence, joined by Justice Sotomayor, ventured an answer, and it tracks the argument this Comment makes in Section IV.C.3 almost exactly: because the warrant here said “only that officers would *attempt* to narrow down the list” at Steps Two and Three without ever requiring it or specifying how, it left too much discretion to the officers executing the order, handing them a broad, open-ended investigative authority precisely the kind the Fourth Amendment condemns.³⁶¹ That view drew only two votes; the five-Justice majority took no position on how the reasonableness inquiry should come out, and the three dissenters never reached it at all.³⁶²

This is not a gap the remand will close quickly, or for anyone outside the Fourth Circuit, which is precisely the structural problem that this Comment identifies. Whatever standard emerges on remand will bind one circuit, will take years to arrive, and will be tethered to the facts of a single 2019 bank robbery rather than to the geofence warrants magistrates approve nationwide. Nothing in the Court's opinion tells the officers behind these warrants how many narrowing steps are enough or what a warrant must say before a magistrate may sign it. The Supreme Court's Opinion confirms that geofence warrants implicate the Fourth Amendment; by its own terms, it cannot tell law enforcement how to draft one that survives it.³⁶³ That is exactly the gap the Geofence Location Data Access Act is built to close, not by waiting for the reasonableness question to percolate circuit by circuit over the coming years, but by codifying, for every magistrate and officer in the country, the step-by-step probable cause findings, narrowing criteria, and sensitive-location protections that eight years of *Carpenter* and now *Chatrie* have left to case-by-case improvisation.

Provided in the attached Appendix is the full text of the proposed bill.

VI. CONCLUSION

Applying the good-faith exception to geofence warrants represents a significant drift from the Fourth Amendment's principles, allowing

360. *Id.* at *17.

361. *Id.* at *18 (Jackson, J., concurring) (citation omitted).

362. *Id.* at *17–18, *27.

363. *See generally id.* (holding that accessing Location History through a geofence warrant is a Fourth Amendment search, but declining to decide whether the warrant's three-step process satisfied the particularity and probable cause requirements, and remanding that question to the Fourth Circuit in the first instance).

unchecked digital sweeps of data that erode privacy.³⁶⁴ Geofence warrants allow law enforcement to obtain location histories for a large number of people without individualized probable cause or particularized descriptions of which devices to search.³⁶⁵ This ultimately violates the Fourth Amendment's prohibitions against unreasonable searches.³⁶⁶ There is no safe haven in the *Leon* good-faith exception because geofence warrants in practice involve widespread magistrate rubberstamping, delegation of probable cause and particularity determinations to private corporations like Google, and warrants so lacking in constitutional indicia as to preclude reasonable reliance.³⁶⁷ Judicial division only creates constitutional fog, allowing inconsistent application that undermines public trust and the integrity of the Fourth Amendment.

The remedy is not in further litigation but in a legislative decision. The Geofence Location Data Access Act lays out the necessary protections by limiting the use of geofences to serious offenses, capping data collection to twenty-five individuals, mandating step-by-step judicial review with probable cause for each step; prohibiting intrusions into homes, worship sites, or medical facilities; and requiring robust reporting.³⁶⁸ This proposed legislation fixes constitutional defects, closes loopholes created in *Leon*, and prevents judicial abandonment by ensuring technology serves justice rather than undermines it.³⁶⁹ Congress must pass this law promptly to put an end to this digital dragnet, make it clear that there is no waiver of rights just because data is shared, and protect the Fourth Amendment.

364. See generally *United States v. Smith*, 110 F.4th 817 (finding geofence warrants unconstitutional and analogous to colonial writs of assistance, but not suppressing evidence gathered due to a finding of good faith).

365. See *id.* at 824 (noting that for every geofence warrant, Google searches each account in the Sensorvault amounting to a total of 592 million people being searched per warrant).

366. See discussion *supra* Part III (explaining how geofence warrants violate the Fourth Amendment).

367. See discussion *supra* Part IV (arguing why *Leon*'s good-faith exception does not apply to geofence warrants).

368. See *infra* Appendix (proposing legislation that will limit the scope and use of geofence warrants).

369. See *id.*

APPENDIX

A BILL

To regulate the compelled disclosure of geofence location data by electronic service providers, to establish heightened standards for geofence warrants to protect privacy rights under the Fourth Amendment, and for other purposes. Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “Geofence Location Data Access Act of 2026.”

SEC. 2. DEFINITIONS.

In this Act:

- (1) “geofence warrant” means a court order issued pursuant to this Act, authorizing the compelled disclosure of location data from an electronic service provider for devices within a specified geographic area and time period.
- (2) “location data” means any data or information that reveals the past or present physical location of a device, including through global positioning system (GPS) coordinates, Wi-Fi signals, Bluetooth beacons, or elevation measurements, and explicitly includes data stored in databases such as Google’s Sensorvault or equivalent sources maintained by other providers.
- (3) “electronic service provider” means any entity that collects, stores, or processes location data on behalf of users, and such provider shall be deemed an agent of the Government for purposes of the Fourth Amendment when compelled to conduct a search under a geofence warrant.
- (4) “serious offense” means:
 - (A) any felony offense enumerated in Section 2516 of Title 18, United States Code; or
 - (B) any other felony offense involving imminent harm to life or safety, such as murder, kidnapping, terrorism, or drug trafficking exceeding thresholds specified in Section 2516 of Title 18, United States Code.
- (5) “person” means officer or employee of the United States, any state, or political subdivision thereof, and any agency or private entity.

SEC. 3. PROHIBITIONS ON UNAUTHORIZED ACCESS TO GEOFENCE LOCATION DATA.

- (1) OFFENSES—Except as otherwise specifically provided in this Act, any person who:

- (a) intentionally accesses, endeavors to access, or procures any other person to access or endeavor to access, geofence location data without authorization under this Act;
 - (b) intentionally discloses, or endeavors to disclose, to any other person the contents of any geofence location data, knowing or having reason to know that the information was obtained through unauthorized access in violation of this subsection;
 - (c) intentionally uses, or endeavors to use, the contents of any geofence location data, knowing or having reason to know that the information was obtained through unauthorized access in violation of this subsection; or
 - (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any geofence location data, obtained by means authorized by Sections 4 and 5 of this Act,
 - (ii) knowing or having reason to know that the information was obtained through such access in connection with a criminal investigation,
 - (iii) having obtained or received the information in connection with a criminal investigation, and
 - (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation, shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).
- (2) EXCEPTIONS—
- (a) PROVIDER ACTIVITIES—It shall not be unlawful under this Act for an officer, employee, or agent of an electronic service provider, whose facilities are used in the transmission or storage of location data, to access, disclose, or use that data in the normal course of employment while engaged in any activity which is a necessary incident to the rendition of service or to the protection of the rights or property of the provider, except that a provider shall not utilize random monitoring except for mechanical or service quality control checks.
 - (b) ASSISTANCE TO LAW ENFORCEMENT—Notwithstanding any other law, electronic service providers, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to access geofence location data under a geofence warrant issued pursuant to Sections 4 and 5 of this Act, if such provider has been provided with:
 - (i) a court order directing such assistance signed by the authorizing judge; or
 - (ii) a certification in writing by a person specified in Section 4(a) of this Act or the Attorney General of the United

States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any access or the device used to accomplish the access with respect to which the person has been furnished a court order or certification under this Act, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a state or any political subdivision of a State, as may be appropriate. Any such disclosure shall render such person liable for the civil damages provided for in subsection (5). No cause of action shall lie in any court against any provider, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order or certification under this Act.

- (c) CONSENT—It shall not be unlawful under this Act for a person acting under color of law to access geofence location data where such person is a party to the data or one of the parties has given prior consent to such access.
 - (d) NON-GOVERNMENTAL ACCESS—It shall not be unlawful under this Act for a person not acting under color of law to access geofence location data where such person is a party to the data or where one of the parties has given prior consent to such access unless such access is for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any state.
 - (e) EMERGENCY SITUATIONS—Notwithstanding any other provision of this Act, in cases of immediate danger of death or serious physical injury to any person, an electronic service provider may disclose geofence location data without a warrant if the requesting officer certifies in writing that such disclosure is necessary, but the officer must apply for a geofence warrant within forty-eight hours thereafter. If the warrant is denied, the data shall be immediately destroyed and may not be used in any proceeding.
- (3) DIVULGENCE BY PROVIDERS—
- (a) Except as provided in paragraph (b) of this subsection, an electronic service provider shall not intentionally divulge

geofence location data (other than to such provider or an agent thereof) to any person or entity other than an authorized recipient under a geofence warrant.

- (b) An electronic service provider may divulge geofence location data:
 - (i) as otherwise authorized in Section 3(2) or Section 7 of this Act;
 - (ii) with the lawful consent of the affected individual;
 - (iii) to a person employed or authorized, or whose facilities are used, to forward such data as necessary for technical purposes; or
 - (iv) which were inadvertently obtained by the provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4) **PENALTIES—**

- (a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this Section shall be fined under Title 18, United States Code, or imprisoned not more than five years, or both.
- (b) If the offense consists of or relates to the access of geofence location data that is not encrypted or scrambled and is for non-commercial purposes, it is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

(5) **CIVIL ACTIONS—**

- (a) Any aggrieved person whose geofence location data is accessed in violation of this Act may bring a civil action against the violator in a United States district court or appropriate state court.
- (b) In an action under this Act, appropriate relief includes—
 - (i) such preliminary and other equitable or declaratory relief as may be appropriate;
 - (ii) punitive damages in cases of willful or intentional violation; and
 - (iii) reasonable attorney's fees and other litigation costs reasonably incurred.
- (c) The court may use any means within its authority to enforce an injunction issued under this subsection and shall impose a civil fine of not less than \$500 for each violation of such an injunction.

SEC. 4. APPLICATION FOR AN ORDER AUTHORIZING ACCESS TO GEOFENCE LOCATION DATA.

- (1) Each application for an order authorizing or approving the access to geofence location data under this Act shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state

the applicant's authority to make such application. Each application shall include the following information:

- (a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;
 - (b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify the belief that an order should be issued, including:
 - (i) details as to the particular serious offense that has been, is being, or is about to be committed,
 - (ii) a particular description of the nature and location of the geofence from which the location data is to be accessed,
 - (iii) a particular description of the type of location data sought to be accessed,
 - (iv) the identity of the person, if known, committing the offense and whose location data is to be accessed;
 - (c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;
 - (d) a statement of the period of time for which the access is required to be maintained, not exceeding two hours for the geofence time window. If the nature of the investigation is such that the authorization for access should not automatically terminate when the described type of data has been first obtained, a particular description of facts establishing probable cause to believe that additional data of the same type will occur thereafter;
 - (e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to access, or for approval of access to, geofence location data involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and
 - (f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the access, or a reasonable explanation of the failure to obtain such results.
- (2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.
- (3) Upon such application the judge may enter an *ex parte* order, as requested or as modified, authorizing or approving access to geofence location data within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile device authorized by a federal court within such jurisdiction), if the judge determines on the basis of the

facts submitted by the applicant that:

- (a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular serious offense;
 - (b) there is probable cause for belief that particular location data concerning that offense will be obtained through such access;
 - (c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;
 - (d) there is probable cause for belief that the geofence from which, or the place where, the location data is to be accessed is being used, or is about to be used, in connection with the commission of such offense, or is leased to, listed in the name of, or commonly used by such person.
- (4) Each order authorizing or approving the access to geofence location data under this Act shall specify—
- (a) the identity of the person, if known, whose location data is to be accessed;
 - (b) the nature and location of the geofence as to which authority to access is granted;
 - (c) a particular description of the type of location data sought to be accessed, and a statement of the particular offense to which it relates;
 - (d) the identity of the agency authorized to access the data, and of the person authorizing the application;
 - (e) the period of time during which such access is authorized, including a statement as to whether or not the access shall automatically terminate when the described data has been first obtained; and
 - (f) a multi-step process, requiring separate judicial approval for each phase beyond Step 1 (anonymized device counts or lists), with Steps 2 (additional contextual data) and 3 (de-anonymization) requiring individualized probable cause for each device or account.

An order authorizing the access to geofence location data under this Act shall, upon request of the applicant, direct that an electronic service provider, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the access unobtrusively and with a minimum of interference with the services that such provider is according the person whose data is to be accessed. Any provider furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance.

- (5) No order entered under this Section may authorize or approve the access to geofence location data for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct access under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with Section 4 of this Act and the court making the findings required by subsection (1) of this Section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to access shall be executed as soon as practicable, shall be conducted in such a way as to minimize the access to data not otherwise subject to access under this Act, and must terminate upon attainment of the authorized objective, or in any event in thirty days. Access under this Act may be conducted in whole or in part by government personnel, or by an individual operating under a contract with the government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the access.
- (6) Whenever an order authorizing access is entered pursuant to this Act, the order shall require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued access. Such reports shall be made at such intervals as the judge may require.
- (7) The contents of any geofence location data accessed by any means authorized by this Act including Step 1 anonymized device identifiers, Step 2 contextual records, and Step 3 de-anonymized subscriber information shall, to the extent technically feasible, be preserved in a tamper-proof format using encryption, write-once storage, or equivalent integrity controls.
- (8) Applications made and orders granted under this Act shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.
- (9) Within a reasonable time, but not later than ninety days, after the filing of an application for an order of approval under this Act which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to accessed data as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of:

- (a) the fact of the entry of the order or the application;
 - (b) the date of the entry and the period of authorized, approved or disapproved access, or the denial of the application; and
 - (c) the fact that location data was or was not accessed during the period. The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the accessed data, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction, the serving of the inventory required by this subsection may be postponed.
- (10) The contents of any geofence location data accessed pursuant to this Act, or evidence derived therefrom, shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a federal or state court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the access was authorized or approved. This ten-day period may be waived by the judge if they find that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.
- (11) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a state, or a political subdivision thereof, may move to suppress the contents of any geofence location data accessed pursuant to this Act, or evidence derived therefrom, on the grounds that:
- (a) the data was unlawfully accessed;
 - (b) the order of authorization or approval under which it was accessed is insufficient on its face; or
 - (c) the access was not made in conformity with the order of authorization or approval.
- Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the accessed geofence location data, or evidence derived therefrom, shall be treated as having been obtained in violation of this Act. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the accessed data or evidence derived therefrom as the judge determines to be in the interests of justice.
- (12) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under

subsection (9), or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.

- (13) The remedies and sanctions described in this Act with respect to the access to geofence location data are the only judicial remedies and sanctions for nonconstitutional violations of this Act involving such data.

SEC. 5. PARTICULARITY AND SENSITIVE LOCATION PROTECTIONS

- (1) **GEOGRAPHIC AND POPULATION LIMITS**—No geofence warrant may be issued unless the application includes:
- (a) a scaled map of the proposed geofence with radius in meters;
 - (b) an affidavit from the applicant estimating the number of individuals likely present in the area during the requested time window, based on provider density reports, census data, or traffic studies; and
 - (c) a judicial finding that the geofence will affect no more than twenty-five (25) individuals.
- (2) **PROHIBITION ON SENSITIVE LOCATIONS**—No geofence warrant shall authorize access to location data from:
- (a) private residences;
 - (b) places of worship;
 - (c) medical facilities; or
 - (d) parking lots serving any of the above

SEC. 6. REPORTING AND TRANSPARENCY.

- (1) **ANNUAL REPORTS**—In March of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a state, or the principal prosecuting attorney for any political subdivision of a state, shall report to the Administrative Office of the United States Courts:
- (a) the number of applications made and orders issued;
 - (b) the serious offenses involved;
 - (c) the number of devices and individuals affected;
 - (d) instances of false positives or wrongful identifications; and
 - (e) the efficacy of the warrants in securing convictions.
- (2) **PROVIDER REPORTS**—Each electronic service provider shall annually publish aggregated data on geofence warrant requests received, including the number complied with and any motions to quash filed.
- (3) **OVERSIGHT**—The Inspector General of the Department of Justice

shall conduct biennial audits of geofence warrant practices and report findings to Congress.

SEC. 7. EFFECTIVE DATE.

This Act shall take effect 180 days after the date of enactment.