Opting Out of Privacy: *United States v. Chatrie* and the Erosion of Fourth Amendment Protections*

Modern smartphones generate a detailed record of their users' physical movements, often with little awareness from the people carrying them. This Recent Development analyzes the Fourth Circuit's decision in United States v. Chatrie *and its implications for Fourth Amendment privacy in the digital age. The panel majority initially held that a user who opts into Google's Location History voluntarily exposes that data to a third party, eliminating any reasonable expectation of privacy under the third-party doctrine. Although the court later affirmed the judgment en banc on good-faith grounds without resolving the constitutional question, the panel's reasoning remains significant. This Recent Development argues that the panel majority's conception of "voluntary" consent is ill-suited to modern digital environments, where users routinely accept opaque data practices through brief pop-ups and terms of service they rarely read or understand. Treating such consent as a waiver of constitutional privacy protections risks extending the third-party doctrine to vast amounts of sensitive digital information. As smartphones become integral to daily life, the reasoning in* Chatrie *threatens to erode the Fourth Amendment's protection against warrantless digital surveillance.*

INTRODUCTION

As of 2024, ninety-eight percent of Americans own a cell phone, and, of that percentage, nine-in-ten own a smartphone.[1] Generally, this is a positive development: means of communication have broadened and accelerated, accessibility to news and healthcare has increased dramatically, and Americans' overall connectivity has proliferated. In fact, fifteen percent of U.S. adults are "smartphone-only" internet users, meaning they rely on a smartphone rather than home broadband service for internet access.[2] This trend is particularly common among Americans with lower household incomes and lower levels of formal education.[3]

1. *Mobile Fact Sheet*, PEW RSCH. CTR. (Nov. 13, 2024), https://www.pewresearch.org/internet/fact-sheet/mobile/ [https://perma.cc/967S-PGWQ].

2. *Id.*

3. *Id.*

However, for all the benefits that smartphones provide, the average user does not contemplate that, in agreeing to use some of their basic features, they may be signing away a fundamental protection. Nevertheless, the Fourth Circuit's panel decision in *United States v. Chatrie*[4] held that, for millions of smartphone users, the Fourth Amendment right to privacy is not triggered when the government requests and is given a detailed history of a user's movements through smartphone location tracking.[5] More specifically, the panel majority concluded that when a smartphone user opts in to Google's "Location History" feature, they have voluntarily handed over information to a third party such that they have no reasonable expectation of privacy to that data.[6] With no reasonable expectation of privacy, the Fourth Circuit held that a search does not take place when law enforcement obtains a "geofence warrant" for this Location History, and therefore the Fourth Amendment is not implicated.[7]

Then, following a rehearing en banc, the Fourth Circuit walked back its holding. Rather than conclude that accessing Location History does not amount to a search, the court instead held that the good-faith exception to the exclusionary rule applies, obviating a ruling on the constitutionality of accessing Location History without a traditional warrant.[8] However, following the en banc one-sentence majority opinion[9] are over sixty pages of separate opinions, including eight concurrences and one dissent, many of which do discuss the merits of whether a search took place in this case.[10] Against this backdrop, this Recent Development argues that the Fourth Circuit's initial holding—finding meaningful voluntariness in the process of opting into Location History—set a dangerous precedent by allowing law enforcement to access intimate details of one's life based solely on a quick tap on a smartphone. And, in light of the

4. 107 F.4th 319 (4th Cir. 2024), *aff'd en banc*, 136 F.4th 100 (4th Cir. 2025), *cert. granted*, No. 25–112 (U.S. Jan. 16, 2026).

5. *See id.* at 339.

6. *See id.* at 331–32.

7. *See id.* at 332.

8. United States v. Chatrie, 136 F.4th 100, 101 (4th Cir. 2025) (per curiam), *cert. granted*, No. 25–112, 2026 WL 120676 (U.S. Jan. 16, 2026).

9. The new majority opinion states, in full: "The judgment of the district court is AFFIRMED." *Id.* at 101.

10. Specifically, five judges opined in detail about whether a search took place, while the other opinions focused on the application of the exclusionary rule. *Compare id.* at 109–13 (Wilkinson, J., concurring) (analyzing whether a search took place); *and id.* at 113–14 (Niemeyer, J., concurring) (same); *and id.* at 115–30 (Wynn, J., concurring) (same); *and id.* at 130–41 (Richardson, J., concurring) (same); *and id.* at 143–56 (Berner, J., concurring) (same); *with id.* at 101–09 (Diaz, C.J., concurring) (focusing elsewhere); *and id.* at 115 (King, J., concurring) (same); *and id.* at 141–43 (Heytens, J., concurring) (same); *and id.* at 156–62 (Gregory, J., dissenting) (same).

uncertainty provided by the en banc decision, the repercussions of this holding are likely to persist.[11]

This Recent Development proceeds in four parts. Part I provides relevant background on the third-party doctrine and its application to smartphone Location History, as well as a short primer on geofence warrants. Part II examines the facts of *Chatrie*, as well as the panel majority and dissent's reasoning as to why the *Chatrie* defendant did or did not have a reasonable expectation of privacy to his Location History. Part III discusses the en banc decision and its reliance on the good-faith exception to the exclusionary rule. Finally, Part IV explores the immediate implications of both of the Fourth Circuit's decisions, as well as possible consequences that may arise in the future.

I. THE THIRD-PARTY DOCTRINE, *CARPENTER*, AND GEOFENCE WARRANTS

The Fourth Amendment protects a person's right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," and generally requires a warrant before any search or seizure occurs.[12] Though initially rooted in the doctrine of trespass, the Supreme Court eventually acknowledged that "property rights are not the sole measure of Fourth Amendment violations."[13] Instead, Justice Harlan's concurrence in *Katz v. United States*[14] proposed that a "reasonable expectation of privacy" standard should frame whether a search took place, in light of growing electronic device usage.[15] This more flexible standard—quickly adopted by the Supreme Court as one of the primary tests for assessing whether a search took place[16]—considers an individual's own intention to keep something private and whether that

11. While Google has since taken steps to mitigate concerns about using geofence warrants to access Location History, *see infra* note 119 and accompanying text, the use of geofence warrants is not limited to Google products. *See* United States v. Smith, 110 F.4th 817, 821 n.2 (5th Cir. 2024) ("Companies such as Apple, Lyft, Snapchat, and Uber have all received geofence warrant requests.").

12. U.S. CONST. amend. IV.

13. Soldal v. Cook County, 506 U.S. 56, 64 (1992); *see also* Katz v. United States, 389 U.S. 347, 351 (1967) ("[T]he Fourth Amendment protects people, not places.").

14. 389 U.S. 347 (1967).

15. *Id.* at 360–62 (Harlan, J., concurring).

16. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 740 (1979) ("Consistently with *Katz*, this Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action." (first citing Rakas v. Illinois, 439 U.S. 128, 143 (1978); then citing *id.* at 150, 151 (Powell, J., concurring); then citing *id.* at 164 (White, J., dissenting); then citing United States v. Chadwick, 433 U.S. 1, 7 (1977); then citing United States v. Miller, 425 U.S. 435, 442 (1976); then citing United States v. Dionisio, 410 U.S. 1, 14 (1973); then citing Couch v. United States, 409 U.S. 322, 335–36 (1973); then citing United States v. White, 401 U.S. 745, 752 (1971) (plurality opinion); then citing Mancusi v. DeForte, 392 U.S. 364, 368 (1968); and then citing Terry v. Ohio, 392 U.S. 1, 9 (1968))).

expectation of privacy is "one that society is prepared to recognize as reasonable."[17]

While *Katz* certainly marked an expansion of Fourth Amendment protection, a series of subsequent Supreme Court decisions limited this reasonable-expectation framework, particularly through the third-party doctrine.[18] The third-party doctrine arises from the notion that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties,"[19] because that person "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[20] For example, law enforcement may access an individual's bank records without a warrant because that individual has already shared this information with a third party—the bank.[21]

While straightforward in rudimentary disclosures of information, application of the third-party doctrine is undoubtedly more complex in instances of electronic device usage. For example, the Supreme Court's landmark decision in *Carpenter v. United States*[22] held that the third-party doctrine does not apply to historical cell-site location information ("CSLI") obtained by the government "from a third party."[23] Specifically, the Court in *Carpenter* concluded that even though cell-site records are stored by wireless carriers (third parties), "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI."[24] Furthermore, the Court emphasized the "unique nature" and "qualitatively different category" of cell phone location records, in comparison to the technology that existed when the third-party doctrine was established.[25] Unlike collecting the numbers dialed on a person's telephone, the Court reasoned,

17. *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (internal quotation marks omitted).

18. *See Smith*, 442 U.S. at 737–38 (holding that a person does not have a reasonable expectation of privacy to phone numbers they dialed, as the numbers were voluntarily conveyed to the phone company); *Miller*, 425 U.S. at 442–43 (holding that a person does not have a reasonable expectation of privacy to their bank records, as those records were voluntarily exposed to the bank in the ordinary course of business); United States v. Knotts, 460 U.S. 276, 281 (1983) (holding that police did not conduct a search when they used a radio transmitter to track a vehicle traveling on *public* roads during one trip). *But see* United States v. Karo, 468 U.S. 705, 714–16 (1984) (holding that the use of a radio transmitter to surveil activity within a location closed to public view did constitute a search).

19. *Smith*, 442 U.S. at 743–44 (first citing *Miller*, 425 U.S. at 442–44; then citing *Couch*, 409 U.S. at 335–36; then citing *White*, 401 U.S. at 752 (plurality opinion); then citing Hoffa v. United States, 385 U.S. 293, 302 (1966); and then citing Lopez v. United States, 373 U.S. 427, 436 (1963)).

20. *Miller*, 425 U.S. at 443.

21. *Id.* at 442–43.

22. 138 S. Ct. 2206 (2018).

23. *Id.* at 2220.

24. *Id.* at 2217.

25. *Id.* ("[I]n 1979, few could have imagined a society in which a phone goes wherever its owner goes.").

CSLI data "provides an intimate window into a person's life," including their "familial, political, professional, religious, and sexual associations."[26] Therefore, the Supreme Court concluded that acquiring one's CSLI is a search under the Fourth Amendment.[27]

While the Court in *Carpenter* determined that the government's acquisition of CSLI constitutes a search—and therefore requires a warrant—the federal circuits had yet to weigh in on the constitutionality of "geofence warrants" prior to *Chatrie*. Unlike a traditional warrant, a geofence warrant "reverses the process" by allowing law enforcement to begin with a crime, rather than a suspect.[28] Typically, this is accomplished in three basic steps. First, law enforcement will submit a warrant to a provider—such as Google—requesting "an anonymized list of all the [provider's] users within a specific location . . . during a given time."[29] This specified criteria is the "geofence."[30] Second, after reviewing the data from the provider, law enforcement *may* narrow down the list of devices before the provider discloses "*all* the location information for [those] devices."[31] Finally, the provider identifies the accounts associated with the devices that law enforcement deems "relevant to the investigation."[32]

Unsurprisingly, such a powerful tool quickly raised questions about Fourth Amendment implications.[33] Primarily, concern has risen over geofence warrants' expansiveness, intrusiveness, and ability "to sweep in users without probable cause."[34] Thus, an abundance of scholarship has suggested that geofence warrants, by their very nature, are prohibited by the Fourth Amendment.[35] However, the *Chatrie* panel majority insisted that the third-party

26. *Id.* (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

27. *Id.* at 2220.

28. Matthew Bradley, *Search and Seizure of Digital Evidence*, COLO. LAW., Mar. 2024, at 24, 29, https://cl.cobar.org/wp-content/uploads/2024/02/March2024_Features-Criminal.pdf. [https://perma.cc/EYT2-8WXC].

29. *Id.*

30. *See id.*

31. *Id.*

32. *Id.*

33. *See, e.g.*, Wendy Davis, *Warranted Intrusion?*, 106 A.B.A. J. 16, 16 (2020) ("As the use of geofence warrants has grown, so have controversies surrounding them. Defense attorneys argue they're unconstitutional, and prosecutors say their use is a valid and valuable crime-solving technique.").

34. Bradley, *supra* note 28, at 29.

35. *See, e.g.*, Esteban De La Torre, *Digital Dragnets: How the Fourth Amendment Should Be Interpreted and Applied to Geofence Warrants*, 31 S. CAL. INTERDISC. L.J. 329, 329–30 (2022); Haley Amster & Brett Diehl, *Against Geofences*, 74 STAN. L. REV. 385, 385–86 (2022); Shelby Stender, *Circumventing the Fourth Amendment: The Unconstitutional Nature of Geofence Warrants*, 2024 UTAH L. REV. 733, 733 (2024).

doctrine prevents geofence warrants from even coming under the purview of the Fourth Amendment.[36]

II. FACTS AND REASONING IN *UNITED STATES V. CHATRIE*

A. *Facts of the Case*

On May 20, 2019, an armed suspect robbed the Call Federal Credit Union in Midlothian, Virginia, of $195,000.[37] With the suspect fleeing before police arrived, the initial investigation into the robbery—via witness interviews and a review of the bank's security footage—did not reveal the suspect's identity.[38] However, law enforcement soon noticed that the suspect was carrying a cell phone during the robbery and applied for a geofence warrant covering the 150-meter radius of the bank.[39] This request was subsequently granted by the county circuit court.[40]

Following the typical steps of a geofence warrant, Google first provided detectives with the anonymized Location History for all devices within the geofence from thirty minutes before to thirty minutes after the robbery.[41] Under these parameters, Google provided 209 location data points from nineteen accounts.[42] At the second step, detectives "attempt[ed] to narrow down that list" to a smaller number to send back to Google.[43] In this case, detectives narrowed the list down to nine accounts.[44] Google then provided the anonymized location data for those devices, now for the span of one hour before to one hour after the robbery.[45] Critically, this new disclosure of Location History was no longer bounded by the geofence.[46] In other words, the information provided from Google at the second step now spanned more than two hours and showed the Location History of all nine devices during this period, regardless of the

36. *See* United States v. Chatrie, 107 F.4th 319, 330–32 (4th Cir. 2024), *aff'd en banc*, 136 F.4th 100 (4th Cir. 2025), *cert. granted*, No. 25–112 (U.S. Jan. 16, 2026) ("The third-party doctrine therefore squarely governs this case. . . . The government therefore did not conduct a search when it obtained the data.").

37. *Id.* at 324.

38. *Id.*

39. *Id.*

40. *Id.*

41. *Id.*

42. *Id.* at 325.

43. *Id.*

44. *Id.* According to the district court, "It does not appear that [the detective] explained to Google precisely why he requested Step 2 data for these nine particular accounts." United States v. Chatrie, 590 F. Supp. 3d 901, 921 (E.D. Va. 2022).

45. *Chatrie*, 107 F.4th at 325.

46. *Id.*

device's proximity to the bank.[47] These parameters resulted in the production of 680 location data points.[48] At the final step, detectives had the opportunity to once more shorten the list before Google would provide the username and other identifying information for the requested accounts.[49] Detectives narrowed the list to three accounts before Google provided the identifying information.[50] One of the three accounts revealed belonged to Okello Chatrie.[51]

Chatrie was subsequently indicted for the robbery, to which he pleaded not guilty.[52] Chatrie moved to suppress the evidence obtained using the geofence warrant, arguing that a geofence warrant is "a modern-day incarnation of the historically reviled general warrant," which cannot satisfy the probable cause or particularity requirements of the Fourth Amendment.[53] However, the district court denied Chatrie's motion, holding that the good-faith exception to the exclusionary rule rendered the evidence admissible.[54] Nonetheless, the district court concluded that this particular geofence warrant was invalid, finding that it "lacked any semblance of . . . particularized probable cause."[55] Following this, Chatrie entered into a conditional guilty plea and was sentenced to 141 months' imprisonment and three years' supervised release.[56]

On appeal, Chatrie asked the Fourth Circuit to hold that the geofence warrant violated his Fourth Amendment rights and, consequently, that the fruits of the warrant should be suppressed.[57] In a 2–1 decision, the Fourth Circuit affirmed the district court's decision to deny Chatrie's motion to suppress, though not based on the good-faith exception.[58] Instead, the Fourth Circuit held that Chatrie "did not have a reasonable expectation of privacy in two hours' worth of Location History data voluntarily exposed to Google," and

47. *Id.*

48. *Id.*

49. *Id.*

50. *Id.* Once again, the district court noted that "it is not apparent from the record whether [the detective] demonstrated to Google why he requested Step 3 data for these three accounts." *Chatrie*, 590 F. Supp. 3d at 921.

51. *Chatrie*, 107 F.4th at 325.

52. *Id.*

53. Defendant Okello Chatrie's Motion to Suppress Evidence Obtained from a "Geofence" General Warrant at 19, 21, United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022) (No. 3:19cr130).

54. *Chatrie*, 107 F.4th at 325. Though discussed in greater detail in Part III, *infra*, the good-faith exception to the exclusionary rule allows evidence obtained during an unconstitutional search to be admitted at trial if police officers acted with an objectively reasonable belief that their actions were lawful. *See* United States v. Leon, 468 U.S. 897, 922 (1984).

55. *Chatrie*, 590 F. Supp. 3d at 927.

56. *Chatrie*, 107 F.4th at 325.

57. *Id.*

58. *Id.*

therefore the government did not conduct a search when it obtained this information.[59]

B. *Reasoning of the Fourth Circuit Panel Majority*

The panel majority's analysis centered solely on the third-party doctrine. While this inquiry typically considers whether the information sought was voluntarily exposed to a third party, the majority also examined the *nature* of the information sought—a new justification derived from *Carpenter* under which courts must consider how revealing the information is.[60] In Chatrie's case, the majority claimed both rationales applied and worked against Chatrie; thus, he did not have a reasonable expectation of privacy.[61]

Regarding the nature of the information justification, the majority concluded that, if an intrusion into one's whereabouts is "short-term" or of a "single, brief trip," then there can be no reasonable expectation of privacy.[62] More specifically, the majority distinguished the information obtained by the geofence warrant from the "all-encompassing record" of whereabouts at issue in *Carpenter*.[63] Here, the court reasoned, the two hours of Chatrie's location history were "no more revealing than his bank records or telephone call logs."[64] Therefore, the third-party doctrine was deemed applicable.[65]

Under the voluntary exposure rationale, the majority concluded that Chatrie freely gave his location information to Google when he opted into Location History, such that he could not have a reasonable expectation of privacy.[66] While this was a straightforward application of the traditional third-party doctrine, the majority was still required to distinguish Chatrie's case from that in *Carpenter*, where the Supreme Court held that the third-party doctrine did not apply to CSLI.[67] In doing so, the majority first contended that, unlike the use of a cell phone, the use of Location History is not necessary "to participat[e] in modern society."[68] Furthermore, the majority asserted that, unlike CSLI, "Location History data is obtained by a user's affirmative act."[69] In other words, because Chatrie at one point opted in to the Location History

59. *Id.*
60. *Id.* at 330 (citing Carpenter v. United States, 138 S. Ct. 2206, 2206 (2018)).
61. *Id.*
62. *Id.* at 330–31.
63. *Id.* at 330 (quoting *Carpenter*, 138 S. Ct. at 2217).
64. *Id.* at 330–31 (first citing United States v. Miller, 425 U.S. 435, 442 (1976); and then citing Smith v. Maryland, 442 U.S. 735, 742 (1979)).
65. *Id.*
66. *Id.* at 331–32.
67. *See Carpenter*, 138 S. Ct. at 2220.
68. *Chatrie*, 107 F.4th at 331 (quoting *Carpenter*, 138 S. Ct. at 2206).
69. *Id.* at 332.

programming, he "'voluntarily "assume[d] the risk"' of turning over his location information."[70] Concluding that Location History is distinguishable from CSLI, the majority held that Chatrie had no reasonable expectation of privacy; thus, the government did not conduct a search in obtaining his data.[71]

C. *Reasoning of the Fourth Circuit Panel Dissent*

In a thirty-four-page dissent, Judge Wynn characterized the majority's holding as providing the government with "a virtually unrestricted right to obtain the Location Data History of every citizen."[72] At the heart of the dissent was a disagreement over what Fourth Amendment standard *Carpenter* set out. While the majority took a more literal approach in applying *Carpenter*—finding that differences between CSLI and Location History rendered them incomparable—the dissent argued that *Carpenter* announced a broader, factor-based framework.[73] Though the dissent began with a meticulous examination of *Carpenter*'s wording in comparison to the cases that came before it, as well as the legal scholarship backing up this claim,[74] the dissent's clearest evidence of a factor test came from *Carpenter*'s conclusion, which states: "In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection."[75] Therefore, in considering whether Fourth Amendment protections apply, the dissent concluded that each of these factors must be weighed "in their totality, [and] with an eye toward maintaining historical expectations of privacy."[76]

Because summarizing the panel dissent's analysis of each factor would be infeasible, this Recent Development focuses primarily on the voluntariness factor—derived from *Carpenter*'s reference to the "automatic nature of [the information's] collection."[77] In the dissent's view, voluntariness even being a factor is debatable: *Carpenter* concluded that the third-party doctrine did not

70. *Id.* (quoting *Carpenter*, 138 S. Ct. at 2220).

71. *Id.*

72. *Id.* at 339 (Wynn, J., dissenting). In the slip opinion, this dissent was nearly seventy pages long, more than double the length of the majority opinion. *See* United States v. Chatrie, No. 22-4489, slip op. at 36–103 (July 9, 2024), https://cases.justia.com/federal/appellate-courts/ca4/22-4489/22-4489-2024-07-09.pdf?ts=1720549856 [https://perma.cc/Z5Q5-N2DK].

73. *See Chatrie*, 107 F.4th at 345–46 (Wynn, J., dissenting).

74. *See id.*

75. *Id.* at 346 (quoting *Carpenter*, 138 S. Ct. at 2206).

76. *Id.* at 348.

77. *Carpenter*, 138 S. Ct. at 2223. The *Chatrie* dissent concluded that the first four factors—comprehensiveness of the intrusion, the intrusion's breadth and retrospective capabilities, intimacy, and ease of access—all suggest that police obtaining Location History data must obtain a warrant. *Chatrie*, 107 F.4th at 348–56 (Wynn, J., dissenting).

apply "*before* it ever addressed voluntariness."[78] For argument's sake, however, the dissent concluded that "Chatrie's sharing of Location History was *not* meaningfully voluntary," for several reasons.[79] First, like CSLI, Location History, once enabled, is "always generated and collected," but unlike CSLI, the data is automatically conveyed every two minutes.[80] Second, the dissent responded to the majority's argument that two-thirds of Google users have not opted in to Location History by pointing out that with 1.5 billion users of Google worldwide, this logic means that around 500 million people *have* "waived their privacy rights."[81]

Lastly, the dissent argued that "the gloss of an opt-in checkbox" does not "meaningfully inform users that they are surrendering 'a comprehensive dossier of [their] physical movements.'"[82] Specifically, the opt-in pop-up text to Location History simply provides an explanation that data "may be saved and used in any Google service where you were signed in to give you more personalized experiences."[83] It also informs users that their data can be accessed and deleted by users.[84] Following this, the screen provides the options: "NO, THANKS" or a brightly highlighted "TURN ON."[85] Additionally, there is a small expansion arrow that, if tapped, displays more information about Location History but need not be clicked in order to opt in.[86] Therefore, "the pop-up box lacked sufficient information for users to knowingly opt into Location History."[87] Consequently, the dissent concluded that any voluntary action that may have taken place here was not meaningful enough to invoke the third-party doctrine.[88]

D. *The Fifth Circuit's Analogous Case*

One month after the Fourth Circuit initially decided *Chatrie*, the Fifth Circuit weighed in on geofence warrants in a nearly identical case, *United States v. Smith*.[89] In this case, the Fifth Circuit held that individuals *do* have a reasonable expectation of privacy in geofence location data from their cell

78. *Chatrie*, 107 F.4th at 356 (Wynn, J., dissenting) (citing *Carpenter*, 138 S. Ct. at 2219). The dissent went on to state that even if it is a factor, the fact that *Carpenter* discussed it only "in a separate rebuttal section" renders it "the least important factor in the overall analysis." *Id.*

79. *Id.*

80. *Id.* at 357.

81. *Id.* at 357–58.

82. *Id.* at 358–59 (alteration in original) (quoting *Carpenter*, 138 S. Ct. at 2220).

83. *Id.* at 359 (quoting United States v. Chatrie, 590 F. Supp. 3d 901, 911–12 (E.D. Va. 2022)).

84. *Id.*

85. *Id.* (quoting *Chatrie*, 590 F. Supp. 3d at 912).

86. *Id.*

87. *Id.*

88. *See id.* at 361.

89. 110 F.4th 817 (5th Cir. 2024).

phones that is protected by the Fourth Amendment.[90] In making this determination, the Fifth Circuit acknowledged persuasive "parallels between CSLI and Location History data."[91] Expressing many of the same concerns as the dissent in *Chatrie*, the court concluded that "the potential intrusiveness of even a snapshot of precise location data should not be understated"[92] and that "electronic opt-in processes are hardly informed and, in many instances, may not even be voluntary."[93] Therefore, the Fifth Circuit held that law enforcement *did* conduct a search when it sought Location History data from Google, and that the third-party doctrine did not apply.[94]

III. THE FOURTH CIRCUIT'S EN BANC RULING AND THE GOOD-FAITH EXCEPTION

Nearly ten months after the initial panel decision in *Chatrie*, a one-sentence en banc ruling pursuant to petition for a rehearing was handed down: "The judgment of the district court is *AFFIRMED*."[95] This per curiam opinion was joined by fourteen of the fifteen active Fourth Circuit judges, with one dissent provided by Judge Gregory.[96]

Importantly, the district court refrained from determining whether a search occurred and instead decided that the information obtained by the geofence warrant should not be suppressed because the good-faith exception to the exclusionary rule applied.[97] Under the good-faith exception, evidence obtained based on law enforcement's reasonable, good-faith reliance on a search warrant later found to be defective can avoid suppression.[98] This exception developed because excluding evidence when officers reasonably relied on a warrant would not meaningfully deter police misconduct.[99] The district court applied this exception because detectives relied on the approval of prior warrants in the face of novel technology, as "no court had yet ruled on the legality of [geofence warrants]" at the time detectives applied for one.[100]

90. *See id.* at 833. The Fifth Circuit even went a step further, holding that geofence warrants are "categorically prohibited by the Fourth Amendment." *Id.* at 838.

91. *Id.* at 833.

92. *Id.*

93. *Id.* at 835.

94. *Id.* at 836.

95. United States v. Chatrie, 136 F.4th 100, 100 (4th Cir. 2025) (en banc) (per curiam), *cert. granted*, No. 25–112 (U.S. Jan. 16, 2026).

96. *Id.* at 100, 156–62.

97. *See* United States v. Chatrie, 590 F. Supp. 3d 901, 941 (E.D. Va. 2022).

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

99. *See id.* at 920–21.

100. *Chatrie*, 590 F. Supp. 3d at 937–38.

Despite fourteen of the fifteen judges concluding that the good-faith exception applied in this case, every judge except for Chief Judge Diaz weighed in to some extent on whether a search occurred, resulting in a 7–7 split.[101] Chief Judge Diaz concluded instead that a finding of good faith precluded a determination of the existence of a search, cautioning that "judicial modesty sometimes counsels that we not make grand constitutional pronouncements merely because we can."[102]

Notably, two of the most-joined opinions were those of Judge Richardson and Judge Wynn,[103] the authors of the panel majority and dissent, respectively.[104] Therefore, while the new holding itself does not clarify whether accessing Location History is a search, the array of opinions emphasizes the need for a clear answer from the court. Most importantly, with no holding that accessing Location History constitutes a search, law enforcement is free to continue gathering this intimate data without the procedural safeguards afforded by a traditional warrant. In other words, the consequences of the initial majority's holding—particularly regarding meaningful voluntariness—are still likely to be felt.

IV. WHAT THE FOURTH CIRCUIT'S DECISION MEANS FOR SMARTPHONE USERS' REASONABLE EXPECTATION OF PRIVACY

It is unlikely that the Supreme Court in the 1970s contemplated a society in which basic tasks are carried out through digital programs or apps that bombard users with requests to use their data. Similarly, the third-party doctrine—advanced primarily through *Smith*[105] and *Miller*[106]—was developed decades before the internet became as ubiquitous as it is today. Yet as Justice Harlan's reasonable expectation of privacy framework developed in light of growing electronic invasions in the 1960s,[107] this protection should be all the more prevalent in today's digital age. Instead, current precedent on geofence

101. *See generally Chatrie*, 136 F.4th 100 (including the one-line per curiam affirmation of the lower court's judgment, eight concurring opinions, and one dissent, all totaling sixty-two pages of the *Federal Reporter*).

102. *Id.* at 101 (Diaz, C.J., concurring).

103. *See id.* at 115 (Wynn, J., concurring); *id.* at 130 (Richardson, J., concurring).

104. United States v. Chatrie, 107 F.4th 319, 321 (4th Cir. 2024), *aff'd en banc*, 136 F.4th 100 (4th Cir. 2025), *cert. granted*, No. 25–112 (U.S. Jan. 16, 2026); *id.* at 339 (Wynn, J., dissenting).

105. Smith v. Maryland, 442 U.S. 735 (1979).

106. United States v. Miller, 425 U.S. 435 (1976).

107. *See* Katz v. United States, 389 U.S. 347, 362 (1967) (Harlan, J., concurring).

warrants creates an imbalance between law enforcement's technological capabilities and Fourth Amendment doctrine.[108]

A closer look at the opt-in process that Chatrie was presented with exemplifies the modern data use request bombardment. In a test of an Android phone—which is used by roughly forty-seven percent of the U.S. population as of 2024[109]—the user was prompted to opt in to Location History when opening Google Maps for the first time.[110] Notably, nowhere on the pop-up did the words "Location History" appear, but rather, the phrase: "Get the most from Google Maps," along with the options of: "YES I'M IN" or "SKIP."[111] Further, the screen contained the statement: "Google needs to periodically store your location to improve route recommendations, search suggestions, and more" and a button with the phrase "LEARN MORE."[112] The information required to make these improvements is hardly disclosed in this brief sequence such that users have "ample notice about the nature of [Location History]."[113]

Additionally, there is a stark difference between the communications that prompted the creation of the third-party doctrine and the communications that are vulnerable under the doctrine's modern application. While the third-party doctrine's foundational cases focused on less-revealing information available in "business records,"[114] Location History users are opting in to near constant tracking over all of their movements. Even though Location History's primary purpose is to enhance user experience, the average person likely does not contemplate that such detailed, personal information is being stored indefinitely when choosing to opt in. Therefore, to say that users "assumed the risk" that this information could subsequently be turned over to law enforcement is far-fetched.[115]

Location History pop-up consent screens also appear when opening other Google applications, such as Google Assistant, Google Photos, and the Google

108. For a greater discussion of the judiciary's role in maintaining homeostasis between technology and Fourth Amendment protections, see generally Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011).

109. Alexandra Borgeaud, *Subscriber Share Held by Smartphone Operating Systems in the United States from 2018 to 2024*, STATISTA (June 26, 2025), https://www.statista.com/statistics/266572/market-share-held-by-smartphone-platforms-in-the-united-states/ [https://perma.cc/V4EU-C4J8 (staff-uploaded, dark archive)].

110. Defendant Okello Chatrie's Supplemental Motion to Suppress Evidence Obtained from a "Geofence" General Warrant at 15, United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022) (No. 3:19cr130) [hereinafter Supplemental Motion to Suppress].

111. *Id.*

112. *Id.*

113. United States v. Chatrie, 107 F.4th 319, 331 (4th Cir. 2024), *aff'd en banc*, 136 F.4th 100 (4th Cir. 2025), *cert. granted*, No. 25–112 (U.S. Jan. 16, 2026).

114. United States v. Miller, 425 U.S. 435, 440 (1976).

115. *See* Smith v. Maryland, 442 U.S. 735, 745 (1979).

Search app.[116] This results in a "cumulative effect" that Chatrie himself argued leads to users opting in "by accident, out of frustration, or because of a belief that the services will not work otherwise."[117] This reality weakens the panel majority's claim that users have "no reason to think that these added features are somehow indispensable to participation in modern society."[118] Indeed, almost anyone who owns a smartphone can attest that often the easiest way to get around pop-ups is to click anything that makes them go away. Opting in under any of these circumstances is in no way meaningfully voluntary as to override a reasonable expectation of privacy.

The Fourth Circuit's initial holding would have far-reaching implications beyond Google's Location History. In fact, on December 12, 2023, Google announced that the nature of Location History was changing dramatically: rather than being stored on the company's servers, Location History would now be saved only on users' own devices.[119] In other words, data will no longer be "provided" to a third party—arguably rendering geofence warrants through Google moot. While Google did not list any reasons for making this change, the timing of the decision coincided with pending appeals in both the Fourth and Fifth Circuits and amidst the publicity about geofence warrants after they were used to identify and indict individuals who participated in the Capitol riots on January 6, 2021.[120]

However, even if geofence warrants' practicality is now hindered, the panel's broader contention that opting in to Location History is a meaningfully voluntary act could apply whenever a user agrees to an app's terms and conditions, despite Google's policy change. While the claim that few people actually read the terms and conditions before agreeing to something is not novel, that does not make the consequences of such a fact any less significant. To demonstrate how pervasive this issue is, a 2017 study by Deloitte found that, out of 2,000 U.S. consumers, ninety-one percent consent to terms of service without reading them.[121] And, while courts have held that agreements made in

116. Navdeep Kaur Bal, *The Constitutionality of Geofence Warrants*, BERKELEY J. CRIM. L. BLOG (Jan. 18, 2024), https://www.bjcl.org/blog/the-constitutionality-of-geofence-warrants [https://perma.cc/6RXP-Q88J].

117. Supplemental Motion to Suppress, *supra* note 110, at 18.

118. *Chatrie*, 107 F.4th at 331.

119. Marlo McGriff, *Updates to Location History and New Controls Coming Soon to Maps*, GOOGLE: KEYWORD (Dec. 12, 2023), https://blog.google/products/maps/updates-to-location-history-and-new-controls-coming-soon-to-maps/ [https://perma.cc/T4QV-4UA9 (staff-uploaded archive)].

120. *See* Rachel Weiner & Drew Harwell, *Google Location Data Was Used to Find Jan. 6 Rioters. It's Disappearing.*, WASH. POST, https://www.washingtonpost.com/dc-md-va/2024/01/06/jan-6-google-location-warrants/ [https://perma.cc/W3ZN-9YJY (dark archive)] (last updated Jan. 8, 2024).

121. Jessica Guynn, *What You Need To Know Before Clicking 'I Agree' on that Terms of Service Agreement or Privacy Policy*, USA TODAY, https://www.usatoday.com/story/tech/2020/01/28/not-

the small print of terms of service are enforceable,[122] the interests at stake in *Chatrie* reflect constitutional rights.

Take, for example, a situation almost identical to Google's Location History. Apple, like Google, asks users opening an app for the first time whether they want to allow the company to track their activity across other apps.[123] One study discovered that forty-three percent of users "were confused or unclear about what app tracking means."[124] In fact, some participants in the study revealed that they "thought they needed to accept tracking," because they believed that "their location was integral to the functioning of the app."[125] While geofence warrants are most commonly associated with Google, law enforcement is free to request data from other tracking applications. Following the reasoning in *Chatrie*, these Apple users would be found to have no reasonable expectation of privacy, despite being confused about what they were consenting to.

The holding that the third-party doctrine applies in cases of consent pop-ups may also narrow Fourth Amendment protections outside of location tracking technologies. In fact, "tracking" and "data collection"—often used interchangeably—are both means to obtaining sensitive information.[126] Most prominently, concern has risen over the data privacy of apps used to track menstrual cycles in the wake of the overturning of *Roe v. Wade*.[127] The intimate data recorded in these apps can be used to indicate whether someone was pregnant, and for how long.[128] In other words, this data may provide at least circumstantial evidence a particular app user had an abortion. While period tracker and fertility apps faced criticism for their data protection policies prior to the *Dobbs* decision,[129] twelve states as of 2025 have criminalized abortions in

reading-the-small-print-is-privacy-policy-fail/4565274002/ [https://perma.cc/7NRD-HV34 (dark archive)] (last updated Jan. 29, 2020, at 14:21 ET).

122. *See, e.g.*, Meyer v. Uber Techs., Inc., 868 F.3d 66 (2d Cir. 2017) (holding that an arbitration provision contained in Uber's terms of services was enforceable).

123. Univ. of Bath, *Research Shows Mobile Phone Users Do Not Understand What Data They Might Be Sharing*, SCIENCEDAILY (May 13, 2023), https://www.sciencedaily.com/releases/2023/05/230509122057.htm [https://perma.cc/W3FH-SXWX].

124. *Id.*

125. *Id.*

126. *How Apps Track You*, NYU: CYBER SMART GUIDES, https://www.nyu.edu/life/information-technology/safe-computing/checklists-guides/guides/software-hardware/app-tracking.html [https://perma.cc/JNC4-DVVQ].

127. Rina Torchinsky, *How Period Tracking Apps and Data Privacy Fit into a Post*-Roe v. Wade *Climate*, NPR, https://www.npr.org/2022/05/10/1097482967/roe-v-wade-supreme-court-abortion-period-apps [https://perma.cc/9KSF-H4Z4] (last updated June 24, 2022, at 15:06 ET).

128. *Id.*

129. *See* Sara Morrison, *Should I Delete My Period App? And Other Post*-Roe *Privacy Questions*, VOX (July 6, 2022, at 12:50 ET), https://www.vox.com/recode/2022/7/6/23196809/period-apps-roe-dobbs-data-privacy-abortion [https://perma.cc/6F5E-Y2JB (dark archive)].

almost all circumstances.[130] Therefore, even if these apps strengthen their data security policies going forward, users' data may nonetheless be accessible by law enforcement conducting a criminal investigation and invoking the third-party doctrine against users' reasonable expectation of privacy.

In fact, under *Chatrie*, there is nothing stopping the government from going even further. The average U.S. citizen brings their phone wherever they go—doctor's appointments, religious spaces, protests—with no consideration that the government has access to the entire history of their movements. And this issue will likely compound as technology advances. As the panel dissent points out: "New technologies that collect ever-more-intimate data are becoming integral to daily life in ways we could not have imagined even a short time ago."[131] As Americans become more reliant on their devices, the constitutional right to privacy may erode in tandem—an outcome cautioned about over fifty years ago.[132]

CONCLUSION

The Fourth Circuit's decision in *Chatrie* is disconcerting at best and a complete reworking of our notions of privacy under the Fourth Amendment at worst. However, the en banc decision will not be the final say on the issue. On July 28, 2025, Chatrie filed a petition for a writ of certiorari in the Supreme Court of the United States.[133] On January 16, 2026, the U.S. Supreme Court granted certiorari exclusively to decide whether the execution of the geofence warrant in Chatrie's case violated the Fourth Amendment.[134]

In the meantime, however, the legal implications and residual uncertainty from both Fourth Circuit decisions set Fourth Amendment protections on a precarious cliff. As the panel majority itself pointed out: "Roughly one-third of active Google users have enabled Location History."[135] Now—at least within Fourth Circuit states—these users may have unknowingly waived their constitutional right to a reasonable expectation of privacy in their movements. More broadly, the conclusion that the third-party doctrine applied in *Chatrie* opens the door for law enforcement to gain access to the personal and intimate

130. *See* Allison McCann & Amy Schoenfeld Walker, *Tracking Abortion Laws Across the Country*, N.Y. TIMES, https://www.nytimes.com/interactive/2024/us/abortion-laws-roe-v-wade.html [https://perma.cc/X2LD-9AKV (staff-uploaded, dark archive)] (last updated Sep. 8, 2025, at 11:25 ET).

131. United States v. Chatrie, 107 F.4th 319, 373 (2024) (Wynn, J., dissenting).

132. *See* Katz v. United States, 389 U.S. 347, 362 (1967) (Harlan, J., concurring) ("[R]easonable expectations of privacy may be defeated by electronic as well as physical invasion.").

133. Petition for a Writ of Certiorari, Chatrie v. United States, No. 25–112 (July 28, 2025).

134. Chatrie v. United States, No. 25–112 (U.S. Jan. 16, 2026) (granting certiorari).

135. *Chatrie*, 107 F.4th at 323.

details of virtually any smartphone user that agrees to an app's terms and conditions—without the typical assurances the Fourth Amendment provides.

CHLOE H. IURILLO**

** J.D. Candidate, University of North Carolina School of Law. Thank you to Noah Raftogianis, Emma Santizo, and the entirety of the *North Carolina Law Review* board and staff for their thoughtful comments and meticulous edits. Special thanks to my friends and family, especially my parents, for their unwavering support and endless belief in me.