Washington and Lee Law Review Online

Volume 82 | Issue 1 Article 2

10-14-2024

Unfenced: The Fourth Circuit Gives Geofencing Its First Appellate Go-Ahead in *United States v. Chatrie*

Jordan Wallace-Wolf
University of Arkansas at Little Rock William H. Bowen School of Law, jwallacewol@ualr.edu

Unfenced: The Fourth Circuit Gives Geofencing Its First Appellate Go-Ahead in *United States v. Chatrie*

Jordan Wallace-Wolf*

Abstract

In United States v. Chatrie*, the Fourth Circuit issued the first federal appellate opinion on the Fourth Amendment status of geofencing queries. The opinion is significant because geofences present a conceptual challenge to the framework of* Carpenter v. United States*, the reigning Supreme Court precedent on the Fourth Amendment status of digital searches. That opinion held that long-term tracking of a target individual was a search. However, geofencing reveals information about an indeterminate number of individuals for only a short time, in virtue of their being at a target location during a target span of time. Does the reasoning for the former holding in* Carpenter *entail that the latter is a search, too? I argue that the answer is no, unless* Carpenter *is given an ambitious interpretation. The court in* Chatrie *refused to go that far, and so held that the geofence at issue was not a search. I do not celebrate this result. Instead, I think it illustrates the limitations of* Carpenter*, doctrinally speaking, and the need to confront those limitations with eyes open.*

* Assistant Professor, University of Arkansas, Little Rock. Thanks to Terrence Cain, participants in SEALS, Brian Owsley, and Nick Kahn-Fogel.

Table of Contents

INTRODUCTION

Cell phones generate information about the movements of their owners over time, and this information can be easily stored and organized in a database. Such a database can, in turn, support geofencing surveillance, whereby investigators can find out who was where and when just by crafting the appropriate search query.[1]

For example, investigators may ask who was present during a thirty-minute span on the morning of October 27, 2021, at

1. Several introductions to geofencing are helpful. *See* Michael Boldin, *Caught in the Crosshairs? How Geofence Warrants Turn Innocent People into Suspects*, TENTH AMEND. CTR. (May 22, 2024), https://perma.cc/7QEY-VMAY (opinionated but helpful introductory video); *see also* John C. Ellis, Jr., *Google Data and Geofence Warrant Process*, NAT'L LITIG. SUPPORT BLOG FOR FED./CMTY. DEFS. & CJA PRACS. (June 6, 2022), https://perma.cc/9R83-HN3Z (explaining Google collection of location data).

Penny Lane in Layton, Utah;[2] or who was at the United States Capitol Building on January 6, 2021, from 2:00–6:30pm;[3] or who was present at a vandalized Minneapolis AutoZone soon after the killing of George Floyd, from 5:20–5:40pm on May 27th,[4] and more.[5] In each case, the government identifies a spatiotemporal region of interest, asks a database to be queried about this region, and receives a list of whose cell phones were there.[6] The privacy implications of this ability to peer into the past, at a location of choice, are substantial.[7]

Though the preceding examples come from the last three years, geofencing surveillance is older than that.[8] Investigators

---

2. Jeremy Harris, *Layton Police Use Controversial 'Geo-Fence' Warrants to Investigate Property Crimes*, KUTV (May 16, 2022), https://perma.cc/FW3Z-TEJJ (last updated June 29, 2022).

3. *See* United States v. Rhine, 652 F. Supp. 3d 38, 66 (D.D.C. 2023) (discussing defendant's motion to suppress "Google Location History data obtained by the Government pursuant to a 'geofence' warrant").

4. Zack Whittaker, *Minneapolis Police Tapped Google to Identify George Floyd Protesters*, TECHCRUNCH (Feb. 6, 2021), https://perma.cc/HBA8-4YK7.

5. *See, e.g.*, René Kladzyk, *El Paso Police Used a Controversial Surveillance Technology to Crack the Memorial Park Shooting Cold Case*, EL PASO MATTERS (Sept. 23, 2021), https://perma.cc/SY8W-J29W (noting "it was the use of a controversial surveillance technology" that allowed police to locate an alleged shooter); Jake Snow, *Cops Blanketed San Francisco in Geofence Warrants. Google Was Right to Protect People's Privacy*, AM. C.L. UNION N. CAL. (Jan. 7, 2024), https://perma.cc/WLF3-XVUQ (noting "thousands of [geofence] warrants have been issued, but the particular locations searched" are not known); Matthew Guariglia et al., *Geofence Warrants Threaten Civil Liberties and Free Speech Rights in Kenosha and Nationwide*, ELEC. FRONTIER FOUND. (Sept. 10, 2021), https://perma.cc/V5VL-VNND (highlighting that geofences were used to investigate Kenosha rioters and to find a stolen wallet at a Utah hospital).

6. *See, e.g.*, *Rhine*, 652 F. Supp. at 69 (explaining the geofence warrant process where the government obtained lists of devices that Google "calculated were or could have been" at the target location, followed by a review of such lists, before reporting the identifying information to the court).

7. *See* Stephen E. Henderson, *Fourth Amendment Time Machines (and What They Might Say About Policy Body Cameras)*, 18 U. PA. J. CONST. L. 933, 937–38 (2016) (comparing mobile phone companies "tracking all of our movements" to a time machine for law enforcement and expressing concern about such investigation methods' impact on privacy); *see also* Warrant Builder, MAVERICK DATA SYS., https://perma.cc/HDH4-6G3N (last visited Oct. 2, 2024) (noting "one of the main concerns surrounding geofencing is the potential invasion of privacy on unrelated persons").

8. *See* United States v. Medina, 712 F. Supp. 3d 226, 235 (D.R.I. 2024) ("Tower dumps, geofences, cell-site simulators, warrants seeking real-time

have used it at least since 2018,[9] but its legal status is still uncertain because it does not fit neatly into the framework of the Supreme Court's most recent and important Fourth Amendment search case, *Carpenter v. United States*.[10] The fundamental question is whether geofencing is a search that requires a warrant.

At first, starting in 2020, only enterprising magistrate judges noticed the difficulty of this question. They observed that while *Carpenter* involved the sustained tracking of a single, targeted individual, geofences involve only the brief tracking of the indeterminate individuals who *happened to be present* at a target location.[11] In conceptual terms, the cell-site location

---

and historical [cell site location information]: these techniques are not only no longer new, but also are now a standard part of an investigative repertoire.").

9. *See* Whittaker, *supra* note 4 (explaining briefly the increase in geofence warrants since 2018).

10. 585 U.S. 296 (2018).

11. *See In re* Search of Info. Stored at Premises Controlled by Google, No. 20 M 297, 2020 WL 5491763, at *7 (N.D. Ill. July 8, 2020) ("The government's [geofencing] warrant application suffers from overbreadth, lack of particularity, and provides no compelling reason to abandon Fourth Amendment principles in this case."); *see also In re* Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 753 (N.D. Ill. 2020) ("Because the proposed warrant here seeks information of persons based on nothing other than their close proximity to the Unknown Subject at the time of the [illegal activity], the Court cannot conclude that there is probable cause to believe that the location and identifying information of any of these *other* persons contains evidence of the offense."); *In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345, 353 (N.D. Ill. 2020) (explaining the constitutionality of warrants for geofence location data turns on whether the warrant is sufficiently "particular in *time, location, and scope*"); *In re* Search of Info. that Is Stored at Premises Controlled by Google, LLC, 542 F. Supp. 3d 1153, 1158–59 (D. Kan. 2021) (providing notice that "geofence warrant applications must sufficiently address the breadth of the proposed geofence and how it relates to the investigation"); *In re* of Search of Info. that Is Stored at Premises Controlled by Google LLC, No. 21-SC-3217 (GMH), 2021 WL 6196136, at *18 (D.D.C. Dec. 30, 2021) (finding the geofence warrant was compatible with Fourth Amendment principles, as "the government has established probable cause that . . . evidence related to [criminal] activity will be found within [the geofences]" and "it has carefully limited the scope of the geofences" in both location and timeframe); *In re* of Search of Info. that Is Stored at Premises Controlled by Google, No. 2:22-mj-01325, 2023 WL 2236493, at *14 (S.D. Tex. Feb. 14, 2023) (concluding that there was probable cause to believe that evidence of a crime would be found within the geofenced

information ("CSLI") in *Carpenter* was used to conduct long-term, *person-targeted* surveillance, but geofencing is a species of *impersonal, location-targeted* surveillance,[12] and one that need not be especially lengthy or intensive. The rules for the former seem ill-equipped to handle the latter, and the magistrate judges said as much in dicta, expressing concern that geofencing would not be a search under *Carpenter*.[13]

In 2022, Judge Hannah Lauck amplified these concerns. As a federal judge in the Eastern District of Virginia, she authored the first non-magistrate opinion on geofencing queries in *United States. v. Chatrie*.[14] She recognized that the case implicated "the next phase in the courts' ongoing efforts to apply the tenets underlying the Fourth Amendment to previously unimaginable investigatory methods."[15]

Like the magistrate judges before her, Judge Lauck thought this application would be challenging, writing that *Carpenter* "primarily deals with *deep*, but perhaps not *wide*, intrusions into

---

location and the warrant request was "sufficiently particular as to time, location, and scope").

12. Tower dumps are another kind of location-focused surveillance, because they target a location primarily and only consequently reveal *whoever* happens to be at that location at the relevant time. *See* Katie Haas, *Cell Tower Dumps: Another Surveillance Technique, Another Set of Unanswered Questions*, AM. C.L. UNION (Mar. 27, 2014), https://perma.cc/RN7X-77YP (describing cell tower dumps as "the practice of demanding an enormous amount of cell phone location information—anywhere from hundreds to hundreds of thousands of data points—in an effort to identify just a few suspects").

13. Notably, the magistrate judges in these cases, *supra* note 11, were all confronted with cautious investigators who had *gotten warrants*, despite the fact that they arguably did not have to. *See, e.g.*, *In re* of Search of Info. that Is Stored at Premises Controlled by Google, 2023 WL 2236493, at *8 ("[T]his Court, like others which have evaluated geofence warrant requests in the past, is not required to answer the question of whether the obtaining of this Step One geofence information constitutes a search. For now, it is enough that the applicant has sought the Court's issuance of the warrant."). For this reason, no decision was needed on whether geofencing was a search. *Id.* The main issue was whether the warrants were adequate. *Id. See also* Brian Owsley, *The Best Offense Is a Good Defense: Fourth Amendment Implications of Geofence Warrants*, 50 HOFSTRA L. REV. 829, 838–39 (2022) (noting the debate among judges regarding whether obtaining geofence information constitutes a search).

14. 590 F. Supp. 3d 901 (E.D. Va. 2022).

15. *Id.* at 905.

privacy."[16] In the end, she, like the magistrate judges, did not rule on whether geofences were Fourth Amendment searches. Instead, she stuck to the issue before her, which was whether the government's geofence *warrant* was sound.[17]

The trial decision in *Chatrie* was highly influential. It is cited in nearly every subsequent geofencing case, and several tower dump cases.[18] But there have not been that many,[19] and in any event, they followed Judge Lauck in avoiding the issue of whether geofencing was a Fourth Amendment search.[20] Several judges in these cases expressed concern that geofencing would not be a search under *Carpenter*, but their focus was also on the adequacy of the geofencing warrants before them.[21] Many resorted to a *United States v. Leon*[22] good-faith exception to uphold the government's geofence warrants without clarifying what the Constitution requires.[23] Scholarship on geofences has been modest as well, and not all of it deals with whether geofencing is a search.[24] In short, geofencing's status as a Fourth Amendment search is deeply unsettled.

---

16. *Id.* at 926. *See also Carpenter*, 585 U.S. at 396 (Gorsuch, J., dissenting) ("But what distinguishes historical data from real-time data, or seven days of a single person's data from a download of *everyone's* data over some indefinite period of time?").

17. *Chatrie*, 590 F. Supp. 3d at 938–39.

18. *See, e.g.*, United States v. Rhine, 652 F. Supp. 3d 38, 73 (D.D.C. 2023) (calling *Chatrie* "the lone district court case to directly consider the validity of a geofence warrant after issuance").

19. Some of the most important recent decisions are: Price v. Superior Ct. of Riverside Cnty., 310 Cal. Rptr. 3d 520 (Ct. App. 2023); Wells v. State, 675 S.W.3d 814, 823 (Tex. Ct. App. 2023); People v. Meza, 90 Cal. App. 5th 520, 541 (Cal. Ct. App. 2023); Tomanek v. State, 314 A.3d 750, 756 (Md. App. 2024); State v. Contreras-Sanchez, 5 N.W.3d 151, 158 (Minn. Ct. App. 2024).

20. *See, e.g.*, *Price*, 310 Cal. Rptr. at 542–46 (reviewing the constitutionality of a geofence warrant and determining it was supported by probable cause and a "model of particularity").

21. *See* Owsley, *supra* note 13, at 838–39 (noting the debate amongst judges).

22. 468 U.S. 897, 926 (1984).

23. *See* United States v. Carpenter, No. 8:21-CR-309-VMC-MRM, 2023 WL 3352249, at *12 (M.D. Fla. Feb. 28, 2023) (stating good-faith warrants no suppression); United States v. Wright, No. CR419-149, 2023 WL 6566521, at *25 (S.D. Ga. May 25, 2023) (same); People v. Seymour, 536 P.3d 1260 (Colo. 2023) (same).

24. *See* Jordan Wallace-Wolf, *A Fourth Amendment of People and Places: Three Foundational Claims About Geofencing*, MARQ. L. REV.

Or at least it was. Enter the very recent Fourth Circuit opinion in *United States v. Chatrie*,[25] and the two geofencing cases that followed right on its heels: *United States v. Davis*[26] and *United States v. Smith*.[27] Just as Judge Hannah Lauck's opinion was the first by a non-magistrate judge, the Fourth Circuit's opinion is the first federal appellate opinion on the technology. In virtue of being first, but also in virtue of its deep analysis, *Chatrie* has set the agenda for appellate consideration of geofencing in what may become a *United States v. Maynard*[28] moment for a second, post-*Carpenter*, revolution in Fourth amendment law.[29] Even *Smith*, which expressly disagrees with *Chatrie*, does not unseat the latter's reasoning. *Smith* only confirms *Chatrie's* influence and the need for the Supreme Court to resolve the resulting circuit split.[30]

(forthcoming)(manuscript at 16), https://perma.cc/4BCZ-EZH9 (PDF) (noting the limited scholarly discussion of this question); *see also* Owsley, *supra* note 13, at 863–83 (discussing the constitutional issues with geofence warrants themselves); *see generally* Mary D. Fan, *Big Data Searches and the Future of Criminal Procedure*, 102 Tex. L. Rev. 877 (2023); Reed Sawyers, *For Geofences: An Originalist Approach to the Fourth Amendment*, 29 GEO. MASON L. REV. 787 (2022); Haley Amster & Brett Diehl, *Against Geofences*, 74 STAN. L. REV. 385 (2022); Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508 (2021); Mohit Rathi, *Rethinking Reverse Location Search Warrants*, 111 J. CRIM. L. & CRIMINOLOGY 805 (2021); Donna Lee Elm, *Geofence Warrants: Challenging Digital Dragnets*, 35 CRIM. JUST. 7 (2020).

25. 107 F.4th 319 (4th Cir. 2024).

26. 109 F.4th 1320 (11th Cir. 2024). This was the second geofencing case in federal appellate court, but was a much easier case on the facts and hence a less instructive one.

27. 110 F.4th 817 (5th Cir. 2024).

28. 615 F.3d 544 (D.C. Cir. 2010).

29. *See* Matthew Tokson, *The Next Wave of Fourth Amendment Challenges After* Carpenter, 59 WASHBURN L.J. 1, 7 (2020) (noting that the *Carpenter* opinion "suggests the Court's increasing willingness to look beyond the facts of a case to its broader implications for Fourth Amendment privacy"); *Maynard*, 615 F.3d at 549 (inaugurating roughly ten years of scholarly and judicial ferment about the relationship of the mosaic theory to the Fourth Amendment). *See also Seymour*, 536 P.3d at 94 (leading keyword search case in which the dissent cites *Chatrie*).

30. *See Smith*, 110 F.4th at 820, 840 (holding the use of geofence warrants is unconstitutional as a "modern-day general warrant" and noting that "in doing so, we part ways with our esteemed colleagues on the Fourth Circuit").

In the *Chatrie* decision itself, the majority interprets *Carpenter* and concludes that geofencing is not a search.[31] To reach this conclusion, the majority takes a stand on whether *Carpenter* put forward a true factor test, or if the test treats *revealingness*—revealing enough information to create "an intimate window" into the defendant's life—as an *element*.[32] The majority, against a book-length dissent, holds that revealingness is likely an element of the search test in *Carpenter* and that it was not satisfied.[33] Hence, no search.

Despite the dissent, I think the *Chatrie* majority has the better position on the law. Most courts are unlikely to find that a geofence is a search. I say that courts are *unlikely to find* that geofences are searches rather than that they are *not searches* because the law is not settled. *Carpenter* is indeterminate about the legal relevance of the revealingness of the information acquired by the government.[34] So far as the letter of that opinion goes, the *Chatrie* dissent and the majority are on equal footing with regard to the law. Only future rulings by the Supreme Court can decide which side is right.

However, until that time, the more cautious option is to take the majority's view of the law, according to which revealingness is an element or at least element-like in being a very weighty factor.[35] And if judges are inclined to take this cautious view, then most geofences will not be searches, given their nature as "wide" but not "deep."[36] In Part II, I illustrate this point by addressing the vigorous dissent of Judge Wynn. I

---

31. *See* United States v. Chatrie, 107 F.4th 319, 330 (finding, in reliance on *Carpenter*, that because "Chatrie did not have a reasonable expectation of privacy in the two hours' worth of Location History data that law enforcement obtained from Google" the government "did not conduct a search by obtaining it").

32. *Id.* at 330–31.

33. *See id.* at 331 (explaining "[a]ll the government had was an 'individual trip viewed in isolation'" which was "far less revealing than [the information] obtained in . . . *Carpenter*" and therefore did not create a "legitimate 'expectation of privacy,' in the information obtained by the government").

34. *See* Tokson, *supra* note 29, at 6 ("[I]t would be easy for future courts to limit *Carpenter* to its facts.").

35. *See Smith*, 110 F.4th at 834 n.8 (highlighting the Court's concern with information that has "the capability of revealing intimate, private details about a person's life").

36. United States v. Chatrie, 590 F. Supp. 3d 901, 926 (E.D. Va. 2022).

am sympathetic to his skeptical attitude toward geofences, but I nonetheless argue that his arguments are not convincing. I then show that the *Smith* court's arguments have some of the same weaknesses. My conclusion then is that geofences may be searches under current law, but only if courts are willing to take an ambitious (but not ruled out!) view of the law.

I. BACKGROUND: THE *CHATRIE* CASE AT THE TRIAL AND APPELLATE LEVEL

In this section, I provide some background about the *Chatrie* case, starting just below with the facts developed at the trial court. The record was extensive, so I focus on the facts that are most important for appreciating the case's Fourth Amendment significance. I then discuss the disposition of the case at the trial and appellate court levels, focusing on their legal conclusions with respect to geofencing queries.

The facts of the crime under investigation in *Chatrie* are simple. A bank robbery took place on May 20, 2019, around 4:52pm, at a federal credit union in Midlothian, Virginia.[37] The bank robber brandished a firearm, took $195,000, and left on foot.[38]

More important is how the government went about investigating this otherwise garden-variety bank robbery. After traditional investigation turned up no leads, the government requested and received a warrant asking Google to pose a query to its Sensorvault database and to provide the results to the government, under a specified procedure outlined below.[39] I will refer to this warrant as a geofence warrant and I will refer to querying a database of location information as geofencing. Note that the facts I recount below were true at the time of decision. Some have changed. For example, Google has taken actions to

37. *Id.* at 905.
38. *Id.* at 906.
39. *Id.* at 917.

limit the collection of data in the Sensorvault,[40] though other avenues for geofencing remain open.[41]

Google tracks the location of user devices over time. [42] One database of such data, the Sensorvault, is populated only with information gained through Google's Location History function.[43] Location History is "off by default."[44] The user can opt in to Location History in settings or at the prompting of a Google application.[45] Once turned on, Google is "always collecting" data, even "if the person is not doing anything at all with his or her phone."[46] The data collected by Location History can be paused or deleted, the deletion is designed to be "difficult enough that people won't figure . . . out" how to do it.[47] Okello Chatrie turned on Location History prior to the robbery.[48] Hence, information about the location of his device was being collected when it took place.

Querying the Sensorvualt is a three-step process.[49] At Step 1, investigators present Google with the geofence warrant, which specifies the parameters of the desired geofence, i.e., the area that it covers and the time span it ranges over.[50] Conceptually, these parameters specify a temporal and spatial

---

40. Andy Greenberg & Lily Hay Newman, *Security News This Week: Google Just Denied Cops a Key Surveillance Tool*, WIRED (Dec. 16, 2023), https://perma.cc/JV2K-H5L9; Zack Whittaker, *Google Moves to End Geofence Warrants, a Surveillance Problem It Largely Created*, TECHCRUNCH (Dec. 16, 2023), https://perma.cc/37G2-XG5J.

41. *See* Wallace-Wolf, *supra* note 24 and accompanying text.

42. Jennifer Lynch, *Google's Sensorvault Can Tell Police Where You've Been*, ELEC. FRONTIER FOUND. (Apr. 18, 2019), https://perma.cc/4VTQ-8E2V.

43. Google collects location data through its web and app activity, but it is not in the Sensorvault and so unavailable to law enforcement. *Chatrie*, 590 F. Supp. 3d at 909.

44. *Id.* at 908.

45. *Id.* at 908–09.

46. United States v. Chatrie, 590 F. Supp. 3d 901, 909 (E.D. Va. 2022).

47. *Id.* at 913.

48. *Id.* at 911.

49. *Id.* at 914. *See also supra* note 1 and accompanying text. For a comprehensive summary of the warrant process, *see* United States v. Rhine, 652 F. Supp. 3d 38, 69 (D.D.C. 2023); United States v. Smith, No. 3:21-cr-107-SA, 2023 WL 1930747, at *2 (N.D. Miss. Feb. 10, 2023); Amster & Diehl, *supra* note 24, at 404–05.

50. *Chatrie*, 590 F. Supp. at 915.

region to "catch" or "fence" anyone who was present at a certain time.

In response to the parameters provided by the government, Google searches all of the data in the Sensorvault database in order to determine which records are responsive.[51] The records are de-identified using an arbitrary number in place of actual data about the relevant subscriber or user.[52] Although Google does not impose any specific restrictions on the geofence size or duration, the Google data specialist may consult with law enforcement to arrive at a mutually acceptable search scope.[53]

At Step 2, the government reviews the de-identified data.[54] It may choose to obtain additional data about particular devices "*beyond* the time and geographic scope of the original request."[55] This additional information is used to contextualize the presence of that user in the search parameters.[56] For instance, the user who is in the search parameters but was found to be passing through at a high rate of speed may be eliminated as unrelated to the investigation.[57] "Google has no firm policy as to precisely when a Step 2 request is sufficiently narrow. But if law enforcement requests a lower number of devices from Step 1 to Step 2, this, to some extent, demonstrates to Google that law enforcement has tailored the data it seeks."[58]

Finally, in Step 3, the government may compel Google to provide identifying information for some of the devices that are found to be responsive to the search parameters.[59] This is how a particular flesh and blood person is connected to the data, and hence how their presence in the geofence becomes known.[60]

---

51. *Id.*

52. *See id.* at 915 n.19.

53. *Id.*

54. *Id.* at 916.

55. *Id.*

56. United States v. Chatrie, 590 F. Supp. 3d 901, 916 (E.D. Va. 2022).

57. *Id. See, e.g.*, State v. Contreras-Sanchez, 5 N.W.3d 151, 158 (Minn. Ct. App. 2024) (explaining that a "device passing through the geofence via the road" in a rural area was "immediately distinguishable" from the device that provided location data at the site of the evidence of the crime).

58. *Chatrie*, 590 F. Supp. 3d at 916 (internal quotations omitted).

59. *Id.*

60. *See id.* (explaining that "account-identifying information includes the name and email address associated with the account" (internal quotations omitted)).

Notably, features of the geofence may permit the government to infer the identity of the subscriber connected with a device found in the geofence, even without Google providing that information.[61]

The geofence requested in the *Chatrie* warrant covered a circle centered near the southeastern corner of the credit union that was robbed.[62] The diameter of the circle was 300 meters, which was sufficient to cover the credit union and a portion of a nearby parking lot and church.[63] Note that when the margin of error for Sensorvault data is taken into account, it is possible that the geofence query, though not inclusive of them by its express terms, nevertheless identified devices that were outside the geofence, such as in a nearby Ruby Tuesday, storage building, or apartment complex.[64] The geofence query returned devices in the requested space for the hour-long span from 4:20 PM to 5:20 PM on the day of the robbery.[65]

In response to the warrant, Google produced 210 individual location points distributed across nineteen users who were inside the geofence.[66] At first, the government requested additional information beyond the parameters of the geofence for all nineteen users.[67] However, upon consultation with Google, the government narrowed this request down to nine and then, of those nine, requested identifying information for three accounts, one of which belonged to the defendant.[68] No magistrate's approval was sought before obtaining this additional information.[69] Subsequently, the government contacted Google requesting additional phone number

61. *See id.* at 923–24 (describing the process whereby a defense expert was able to make a probable identification of an individual based upon a search of public records cross referenced against Step 2 data).

62. *See id.* at 919 (providing a visual aid).

63. *See id.* at 922 (showing a diagram of the relevant area).

64. *Id.* at 923.

65. *Id.* at 919. Note that the Fourth Circuit's opinion often refers to two hours of data. *See* United States v. Chatrie, 107 F.4th 319, 325 (4th Cir. 2024) ("Chatrie did not have a reasonable expectation of privacy in *two hours'* worth of Location History data voluntarily exposed to Google." (emphasis added)). The reason for the discrepancy is unclear.

66. United States v. Chatrie, 590 F. Supp. 3d 901, 920–21 (E.D. Va. 2022).

67. *Id.* at 920.

68. *Id.* at 921, 924.

69. *Id.* at 921.

information for one of the revealed accounts, outside of the parameters of the warrant.[70] Google did not provide this information.[71]

The defendant, Okello Chatrie, was subsequently charged with forced accompaniment during an armed credit union robbery and using a firearm in the course of a crime of violence.[72]

A. *The Eastern District of Virginia*

In the trial court, Chatrie sought suppression of the results of the geofence.[73] Judge Lauck ultimately denied this motion on *Leon* good-faith exception grounds,[74] but, commendably, not before at least opining on whether there is reasonable expectation of privacy in the data the government sought, and on whether the warrant was constitutional in its scope.[75]

With regard to whether the geofence intruded on reasonable expectations of privacy, Judge Lauck expressed concern that "current Fourth Amendment doctrine may be materially lagging behind technological innovations."[76] She also wrote that "the Court is disturbed that individuals other than criminal defendants caught within expansive geofences may have no functional way to assert their own privacy rights."[77] Ultimately, she concluded that the "analysis of geofences does not fit neatly within the Supreme Court's existing . . . doctrine as it relates to technology."[78]

With regard to the constitutionality of the warrant itself, she held that it was overbroad, given the evidence that the

---

70. *Id.* (explaining that this additional request for information would have been "an unauthorized Step 4").

71. *Id.* at 921–22.

72. *Id.* at 924.

73. *Id.*

74. *See id.* at 937 ("Despite the warrant failing under Fourth Amendment scrutiny, the *Leon* good faith exception shields the resulting evidence from suppression.").

75. *See id.* at 927–36 (performing analysis on the Fourth Amendment questions).

76. *Id.* at 925.

77. *Id.* at 926.

78. *Id.* at 926.

government possessed.[79] This was for two reasons. One is that the warrant "swept in unrestricted location data for private citizens who had no reason to incur Government scrutiny."[80] In expounding on this reasoning, Judge Lauck cited *Ybarra v. Illinois*[81] and its Fourth Circuit progeny, *Owens* ex rel. *Owens v. Lott*,[82] for the proposition that police may not search someone just because of their "mere propinquity" to the scene of a crime.[83] Instead, she wrote, "warrants . . . that authorize the search of every person within a particular area must establish probable cause to search every one of those persons."[84] This invocation of *Ybarra* in support of this standard has been influential,[85] but also heavily criticized.[86]

---

79. *See id.* at 929 ("[I]t is difficult to overstate the breadth of this warrant, particularly in light of the narrowness of the Government's probable cause showing."). *See also* United States v. Hurwitz, 459 F.3d 463, 473 (4th Cir. 2006) ("The Fourth Amendment requires that a warrant be 'no broader than the probable cause on which it is based.'" (quoting United States v. Zimmerman, 277 F.3d 426, 432 (3d Cir. 2002))).

80. United States v. Chatrie, 590 F. Supp. 3d 901, 930 (E.D. Va. 2022).

81. 444 U.S. 85 (1979).

82. 372 F.3d 267 (4th Cir. 2004).

83. *Chatrie*, 590 F. Supp. at 928 ("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." (quoting Ybarra v. Illinois, 444 U.S. 85, 91 (1979))).

84. *Id.* at 927.

85. *See, e.g.*, Amster & Diehl *supra* note 24, at 424 (noting the similarity between the search in *Ybarra* and the capture of a Google user's data within a geofence); *In re* Search of Info. Stored at Premises Controlled by Google, No. 20 M 297, 2020 WL 5491763, at *18 (N.D. Ill. July 8, 2020) (concluding that the Fourth Amendment will not tolerate agents using discretion to select specific cellular phones from which to seek information); Donna Lee Elm, *supra* note 24, at 11 (citing *Ybarra* for the proposition that "particularization" is not provided by prescribing a search to certain devices within a specific area during a specified period). Moreover, any argument that the particularization is provided by limiting the search to devices within a specific time frame and geographical area fails under a "mere presence" principle. Ybarra v. Illinois, 444 U.S. 85, 95 (1979) (quoting United States v. Di Re, 382 U.S. 581, 587 (1948)).

86. *See* Wallace-Wolf, *supra* note 24; Orin Kerr, *The Fourth Amendment and Geofence Warrants: A Critical Look at U.S. v. Chatrie*, LAWFARE (Mar. 12, 2022), https://perma.cc/6CKL-LBYN (presenting criticism of Judge Lauck's reasoning); *In re* Warrant Application for Use of Canvassing Cell-Site Simulator, 654 F. Supp. 3d 694, 709 (N.D. Ill. 2023) (finding the *Ybarra* analogy to be inapplicable to this cell-site case).

The second is that the size of the geofence was grossly disproportionate given that the government knew exactly where the crime was committed.[87] "[L]aw enforcement simply drew a circle with a 150-meter radius that encompassed the Bank, the entirety of the Church, and the Church's parking lot."[88]

B. *The Fourth Circuit Court of Appeals*

The Fourth Circuit upheld Judge Lauck's decision not to suppress the results of the geofence query, by a split opinion of two to one.[89] Judge Richardson and Judge Wilkinson[90] were in the majority and Judge Wynn[91] dissented.[92]

Fortunately for the development of the law in this area, the majority did not affirm Judge Lauck on the basis of the *Leon* good-faith doctrine.[93] Instead, the court provided some analysis regarding the Fourth Amendment status of geofencing. Specifically, it held that "Chatrie did not have a reasonable expectation of privacy in two hours' worth of Location History data voluntarily exposed to Google. So, the government did not conduct a search when it obtained this information from Google."[94] Chatrie did not have a reasonable expectation of privacy in his Location History data because the latter was

87. *See Chatrie*, 590 F. Supp. 3d at 930 ("[T]his [warrant] captured location data for a user who may not have been remotely close enough to the Bank to participate in or witness the robbery.").

88. *Id.*

89. United States v. Chatrie, 107 F.4th 319, 321 (4th Cir. 2024).

90. Richardson, Julius Ness, *History of the Federal Judiciary, Judges*, FED. JUD. CTR., https://perma.cc/6C7Q-95BN (last visited Sept. 6, 2024) (indicating Judge Richardson was appointed by President Trump); Wilkinson, James Harvie III, *History of the Federal Judiciary, Judges*, FED. JUD. CTR., https://perma.cc/4SES-ZDXX (last visited Sept. 6, 2024) (documenting that Judge Wilkinson was appointed by President Reagan).

91. Wynn, James Andrew, Jr., *History of the Federal Judiciary, Judges*, FED. JUD. CTR., https://perma.cc/P28S-L4PY (last visited Sept. 6, 2024) (showing that Judge Wynn was appointed by President Obama).

92. *Chatrie*, 107 F.4th at 321.

93. *Id.* at 326 ("We agree that the motion should be denied, but for a different reason: Chatrie did not have a reasonable expectation of privacy in two hours' worth of Location History data voluntarily exposed to Google.").

94. *Chatrie*, 107 F.4th at 325; *see id.* at 339 ("We hold that the government did not conduct a Fourth Amendment search when it accessed two hours' worth of Chatrie's location information that he voluntarily exposed to Google.").

governed by the third-party doctrine.[95] When this doctrine applies, a defendant has no "legitimate expectation of privacy" in information about him that is held by a third-party which, in this case, is Google.[96]

To decide whether the third-party doctrine applied, the majority looked primarily to *United States v. Carpenter*,[97] but also to *United States v. Jones*,[98] and *Leaders of a Beautiful Struggle v. Balt. Police Dep't*,[99] neither of which was a third-party case. In a compressed bit of reasoning, the court concluded that the emphasis of *Carpenter*, understood through *Jones* and *Beautiful Struggle*, was on the government's long-term reliance on a deeply revealing dataset that was gathered involuntarily.[100] Hence, whether the doctrine applies, the majority said, turns on two issues: the degree to which the information *sought* implicates privacy, and how voluntarily that information was disclosed to the third-party.[101]

In just seven paragraphs (with more analysis coming later, in a section dedicated to addressing the dissent), the court reasoned that both of these considerations weighed decisively in favor of applying the doctrine.[102] The majority in this section just touches on the first issue—the degree to which the information sought implicates privacy.[103] It simply held that the information sought about the defendant was decisively different than that in *Jones*, *Carpenter*, or *Beautiful Struggle*, all of which involved

95. *Id.* at 332.

96. *Id.* at 326 (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).

97. 585 U.S. 296 (2018).

98. 565 U.S. 400 (2012).

99. 2 F.4th 330 (4th Cir. 2021).

100. *See* United States v. Chatrie, 107 F.4th 319, 328–29 (4th Cir. 2024); *id.* at 328 ("The Court thus explained that CSLI provides law enforcement 'an all-encompassing record of the holder's whereabouts' over that period . . . . Such access—at least, to 7 days' worth of CSLI—invades the reasonable expectation of privacy individuals have 'in the whole of their physical movements.'" (citing Carpenter v. United States, 585 U.S. 296, 311, 310 n.3 (2018))).

101. *Chatrie*, 107 F.4th at 330 ("*Carpenter* identified two rationales that justify applying the third-party doctrine . . . ."). *See also* Carpenter v. United States, 585 U.S. 296, 313–15 (2018) (employing language similar to the language used by the majority in *Chatrie*).

102. *Chatrie*, 107 F.4th at 330–33 (4th Cir. 2024).

103. *Id.*

long-term location tracking over days.[104] Many other courts have drawn this distinction in the context of discussing geofencing.[105]

With regard to voluntariness, the court found that Chatrie provided his location information to Google voluntarily.[106] He was informed about his options.[107] He chose, through an "affirmative act," to opt in to his data being collected,[108] and opting out would not have deprived him of something that was "indispensable to participation in modern society,"[109] as using a cell phone was found to be in *Carpenter*.[110] Notably, the majority's arguments here are strikingly formalistic, painting the defendant's accession to Google's insistent and blipped description of its Location History service as an informed and deliberate act.[111] This description of what happened is highly contestable.[112]

The dissent, in stark contrast to the majority's brevity, offers a lengthy dissertation on the Fourth Amendment's

---

104. *See id.* at 331 ("The information obtained was . . . far less revealing than that obtained in *Jones*, *Carpenter*, or *Beautiful Struggle* . . . .").

105. *See In re* Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 736 (N.D. Ill. 2020) ("The Amended Application presents a different factual setting than did *Carpenter* and *Jones*, in that the Amended Application targets a 45-minute window on three specific days, whereas *Carpenter* involved at least seven days of data and *Jones* involved 28 days . . . ."); *In re* of Search of Info. that Is Stored at Premises Controlled by Google, No. 2:22-mj-01325, 2023 WL 2236493, at *8 (S.D. Tex. Feb. 14, 2023) ("Additionally, this situation is different from *Carpenter* and *Jones* because the time period involved in this warrant is much more brief . . ."). *See also* Sanchez v. Los Angeles Dep't of Transp., No. CV 20-5044-DMG (AFMx), 2021 WL 1220690, at *3 (C.D. Cal. Feb. 23, 2021) (applying the temporal analysis seen in *Jones*), *aff'd*, 39 F.4th 548 (9th Cir. 2022).

106. *See Chatrie*, 107 F.4th at 337 ("Here, we find that Chatrie—unlike Carpenter—did voluntarily expose his Location History to Google.").

107. *Id.* at 331 ("Google provides users with ample notice about the nature of [the Location History] setting.").

108. *Id.* at 332.

109. *Id.* at 331.

110. *See* United States v. Chatrie, 107 F.4th 319, 331 (4th Cir. 2024) ("*Carpenter* found that it is impossible to participate in modern life without a cell phone. But the same cannot be said of Location History.").

111. *See id.* at 329 (painting the defendant's conduct as informed and deliberate).

112. Matthew Tokson, *The Fourth Circuit Approves Warrantless Location Tracking Via Google Apps, Misunderstands How Location Tracking Works*, DORF ON LAW (July 15, 2024), https://perma.cc/L5D5-UURL.

application to new technologies. Specifically, Judge Wynn argues that *Carpenter* replaced the third-party doctrine with a "multifactor test to be used to determine whether a government intrusion using digital technologies constitutes a search."[113] The relevant factors are the degree to which the nature of the data collected is: comprehensive, retrospective, intimately revealing, easily accessible, and voluntarily conveyed to others.[114] Applying this framework, the dissent concluded that a Fourth Amendment search took place.[115] The dissent also thought that the geofence warrant was unconstitutional.[116]

II. THE SIGNIFICANCE OF THE FOURTH CIRCUIT DECISION

In this Part, I discuss the Fourth Circuit opinion in *Chatrie*, with the goal of surfacing its significance for the question of whether geofencing is a Fourth Amendment search (and so, whether it presumptively requires a warrant). In the course of my discussion, I will distinguish two aspects of *Carpenter* and conclude that the majority's way of reconciling them is plausible and likely to be followed.

Note that I do not think that the majority's holding is, from a policy or normative perspective, a good result, and a different approach could avoid it, but I will not argue those points here.[117] Instead, I will focus on what this decision says about the Fourth Amendment's future for geofencing under current Supreme Court precedent.

Given this focus, the third-party doctrine will be a distraction. This is because the third-party doctrine is not always applicable to the kinds of surveillance that skirt *Carpenter's* holding—those that are "wide" but not "deep."[118] In

113. *Chatrie*, 107 F.4th at 340–44.

114. *See id.* at 346 (enumerating the relevant factors).

115. *See id.* at 361 ("Because the balance of the *Carpenter* factors shows that Location History is qualitatively different from the records that police could traditionally obtain without a warrant, Chatrie had a reasonable expectation of privacy in his Location History data, and the government conducted a search by accessing it.").

116. *See id.* at 362 (Wynn, J., dissenting) (explaining that the geofence warrant was unconstitutional).

117. *But see generally* Jordan Wallace-Wolf, *supra* note 24.

118. *See* United States v. Chatrie, 590 F. Supp. 3d 901, 926 (E.D. Va. 2022) (discussing the implications of the third-party doctrine).

other words, sometimes the third-party "off ramp" simply will not be available, in which case, the constitutionality of the government's surveillance will have to addressed directly.

To illustrate, imagine that CSLI becomes highly accurate such that police use it to conduct geofencing searches like those currently accomplished with Google's Location History. In this world, investigators might ask phone carriers which of their subscribers were present in a particular area during a particular span of time. Such a scenario would be almost exactly like *Carpenter* except that it would not target a particular person over the long term, but rather a particular place over the short term. In this hypothetical, it seems that the third-party doctrine would be just as irrelevant as it was in *Carpenter* (which held that CSLI records are created involuntarily and are "unique").[119] So, whether the government conducted a search in the hypothetical would turn solely on the significance of short-versus long-term tracking.[120]

To be sure, *Chatrie is* a third-party case, but the Fourth Circuit opinion includes plenty of analysis about how to apply *Carpenter* to short-term surveillance.[121] This is the part of the opinion that I want to explore.

A. *The Record/Revealingness Distinction in* Carpenter *and Lower Courts*

To explore it, it is worth briefly distinguishing two lines of reasoning in *Carpenter*. They pertain to two moments in the life of a database. First, the database is created, which is accomplished by the creation and organization of records of a certain kind, e.g., location information taken from a phone over time.[122] Then, later, some of the records may be requested.[123]

---

119. *See* Carpenter v. United States, 585 U.S. 296, 297 (2018) (holding that cell-site records are unique).

120. *See id.* at 309–10 (discussing the unique nature of CSLI).

121. *See* United States v. Chatrie, 107 F.4th 319, 330–33 (4th Cir. 2024) (explaining the application of *Carpenter*).

122. *See Carpenter*, 585 U.S. at 300–02 (discussing the storage of location information).

123. *See id.* at 305 (touching upon the requesting of cell-site records).

The database may be queried with some search parameters, e.g., *those records that concern this place during this time span*.[124]

Carpenter sometimes focuses on the first—on the *kind* of record that can be requested by the government from a database, and sometimes on the second—on the *revealingness of the request* that the government makes of the database that houses those records (or the revealingness of the records they actually receive).[125] I will refer to this distinction as the *record/revealingness distinction*. Boiled down, this distinction is one between the kind of records that the government may request in its investigations generally, and on the quantity of those records that the government actually requests in a particular investigation.

Let me illustrate this point with some quotations. The majority in *Carpenter* analyzes the case through a records lens when they write that cell phone location information is "detailed, encyclopedic, and effortlessly compiled";[126] that it is "a qualitatively different category" of record than "telephone numbers and bank records";[127] that cell phone location records are "unique";[128] that cell phone location information is collected, as a matter of course, about a huge swath of the population;[129] that "this sort of digital data—personal location information maintained by a third party—does not fit neatly under existing precedents";[130] that CSLI grants the government "the ability to chronicle a person's past movements through the record of his cell phone signals";[131] and that it presents "even greater privacy concerns than . . . GPS monitoring" given that they are retrospective and can be generated from private areas.[132] In all

124. *See id.* at 301 (describing the time-constrained CSLI requests).
125. *See id.* at 309–16 (focusing on both *kind* and *revealingness*).
126. *Id.* at 309.
127. *Id.*
128. *Id.*
129. Carpenter v. United States, 585 U.S. 296, 311–12 (2018).
130. *Id.* at 306.
131. *Id.* at 309.
132. *Id.* at 297.

of these quotations, the Court is focused on the "nature of the data" requested.[133]

By contrast, the majority in *Carpenter* focuses on the revealingness of the information requested by the government when it writes that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy";[134] that "society's expectation has been that law enforcement agents and others would not . . . catalogue every single movement of an individual's car for a very long period";[135] that "mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts . . . [and] provides an intimate window into a person's life";[136] that with "the 127 days of location data it received, the Government could . . . deduce a detailed log of Carpenter's movements."[137]

Clearly then, the *Carpenter* opinion is concerned with *both* the kind of record the government requests (CSLI) and the revealingness of its request (127 days).[138] Crucially though, the opinion never says how they fit together in a search analysis.[139]

Footnote three of the majority's opinion is the locus of this ambiguity.[140] It reads:

---

133. *See* Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. 357, 374 (2019) (explaining the Court's emphasis on the "nature of the data").

134. *Carpenter*, 585 U.S. at 307.

135. *Id.* at 310.

136. *Id.* at 311.

137. *Id.* at 313.

138. *See id.* at 320 (finding that the acquisition of the CSLI, under the circumstances, was a search).

139. *See* Carpenter v. United States, 585 U.S. 296, 320 (2018) (failing to articulate exactly how the factors fit together in a search analysis).

140. *See Carpenter*, 585 U.S. at 395–96 (Gorsuch, J., dissenting) ("The Court declines to say whether there is any sufficiently limited period of time 'for which the Government may obtain an individual's historical location information free from Fourth Amendment scrutiny.'"); United States v. Howard, 426 F. Supp. 3d 1247, 1255 n.3 (M.D. Ala. 2019), *aff'd*, 858 F. App'x 331 (11th Cir. 2021) ("In *Carpenter*, the Court explicitly refused to answer whether one's 'reasonable expectation of privacy in the whole of his physical movements' extends to shorter periods of time or to other location tracking devices."); *see also* Susan Freiwald & Stephen Wm. Smith, *The Carpenter Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 228 (2018); Ohm, *supra* note 133, at 374. Further, in *Carpenter*, Gorsuch stated "it tells us that access to seven days' worth of information *does* trigger Fourth

> [W]e need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.[141]

The Court partially relies on the amount of information the government requested to decide the case—seven days,[142] without stating how the amount of information requested fits into a search analysis. Without the latter, the former provides little guidance going forward. What about six days of CSLI information? What about eight days of arguably less concerning forms of location-revealing records, such as those created from automatic license plate readers ("ALPR")?[143]

Still, despite this ambiguity, we can distinguish at least three rules that would be logically consistent with *Carpenter's* seven day holding. According to one rule, the government's request of a threshold amount of CSLI-like information—whatever that amount turns out to be—is a necessary *element* for finding that a search occurred.[144] Under this rule, requesting seven days of CSLI information is a search because it is more than whatever the threshold amount is. Whether geofencing is generally a search under this rule would depend on the threshold.

A rule at the other extreme would hold that the scope of the government's request is wholly irrelevant to whether a search

---

Amendment scrutiny—even though here the carrier 'produced only two days of records.'" *Carpenter*, 585 U.S. at 396. Subsequently, Justice Gorsuch posed the following questions: "[w]hy is the relevant fact the seven days of information the government asked for instead of the two days of information the government actually saw?" and "[w]hy seven days instead of ten or three or one?" *Id.*

141. *Carpenter*, 585 U.S. at 310 n.3 (majority opinion).

142. *See id.* at 340 (Gorsuch, J., dissenting) ("The Court suggests that less than seven days of location information may not require a warrant . . . [b]ut the Court does not explain why that is so.").

143. *See* Ohm, *supra* note 133, at 393 ("ALPR generates data that is neither as deep, broad, nor comprehensive as CSLI.").

144. Taylor H. Wilson, Jr., *The Mosaic Theory's Two Steps: Surveying Carpenter in the Lower Courts*, 99 TEX. L. REV. ONLINE 155, 166 (2021) (explaining the interaction, under *Carpenter*, between what would qualify as a search and the number of days' worth of data that the government has collected).

has occurred and that all that matters is the kind of record that is being requested. If the government requests *any amount* of sufficiently CSLI-like information, then a search has occurred. Under this rule, requesting seven days of CSLI records is a search because any request of such records would be a search. If this were the rule, then it seems almost all geofences would be searches, given that they query data that is highly similar to CSLI.[145]

In between these rules lies a third, compromise rule. According to it, the scope of the government's actual request is a factor. It matters, but only in the overall balance. According to this rule, it is conceivable that a very modest request for information could still be a search if the data was highly similar to, or worse than CSLI, judged along dimensions like ease-of-compilation, retrospectivity, intimacy, and so on. Under this rule, requesting seven days of CSLI-like information is a search because requesting that much of that kind of record is enough to weigh, overall, in favor of finding a search. If this were the rule, then whether geofences are searches will depend on how important the request factor is, given that they request information that is similar in kind to CSLI.

Given the Supreme Court's deliberate silence about which of these rules is correct, lower courts have had to make their own way.[146] But no robust pattern has emerged. Matthew Tokson has carefully catalogued the application of *Carpenter* by lower courts, and found that courts decide whether a search has occurred by virtue of the government's collection of databased information with reference to three considerations: the kind of record the government requested (a record-focused factor), how much of it they requested (a revealingness-focused factor), and whether and how the data was disclosed to third-parties.[147]

---

145. *See* Christopher Slobogin, *The Right of the People to Be Secure: Modern Technology and the Fourth Amendment: Suspectless Searches*, 83 OHIO ST. L.J. 953 (2022) (offhandedly suggesting that the *Carpenter* test turns on the nature of the data being queried); David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 71 (2013) (advocating this kind of approach to the Fourth Amendment).

146. *See, e.g.*, People v. Edwards, 97 N.Y.S. 3d 418, 421 (App. Div. 2019) (looking at the volume of data collected in making its search determination).

147. *See* Matthew Tokson, *The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018–2021*, 135 HARV. L. REV. 1790, 1793 (2022) (documenting the three main considerations that lower courts utilize to

However, he cautiously notes that his research does not yet permit conclusions about how exactly these considerations should be an analyzed.[148] Are some factors more important than others? Does one factor operate like an element below a certain threshold, i.e., must the government's request be of a sufficiently large scope for a search to have occurred, regardless of how the other factors weigh?

These and other questions are still open, and they are starkly posed by geofencing, given how little information such surveillance requires.[149] Geofencing is interesting, I will show below, because it forces courts to confront this ambiguity and resolve it, at least until the Supreme Court clarifies *Carpenter*.

B. *The* Chatrie *Decision as a Strong Articulation of a Revealingness Based Approach to Geofencing*

In light of the previous section, consider the majority and the dissent in *Chatrie*. Neither takes the extreme position that the revealingness of the government's information request makes no difference to whether it was a search.[150] Instead, they both agree that it matters.[151] Their principle disagreement is about how much it matters legally, and about how revealing the search in *Chatrie* actually was as a factual matter.[152]

According to the majority, the scope of the government's request is crucially important.[153] It is something close to an

---

determine whether information collected from a database is a search); Matthew Tokson, *The Carpenter Test as a Transformation of Fourth Amendment Law*, 2023 UNIV. ILL. L. REV. 507, 517 (2023) (following up on his Harvard Law Review article).

148. *See id.* at 1831–32 (cautioning about how these considerations should be analyzed).

149. *See* United States v. Chatrie, 107 F.4th 319, 322–23 (4th Cir. 2024) (describing the geofencing process in detail).

150. *See id.* at 332, 340–57 (Wynn, J., dissenting) (explaining that revealingness matters in a search determination).

151. *See id.* (agreeing that revealingness matters in a search determination).

152. *See id.* at 349–60 (disagreeing with the majority's search analysis).

153. *See id.* at 330 (majority opinion) (stating that "only two hours' worth of Chatrie's Location History data" was by no means "an all-encompassing record of Chatrie's whereabouts" (internal quotations omitted)).

element in the *Carpenter* analysis.[154] The revealingness element is satisfied only if the government requests enough information to create "an intimate window into a person's life."[155] If the government does not request enough information to satisfy this intimate window threshold, then there can be no search.[156] Correspondingly, the majority argues that the geofencing information sought by the government did not meet the intimate window threshold.[157]

Judge Wynn, in dissent, argues that the revealingness of the information requested by the government is much less important to the search analysis.[158] Legally speaking, he contends that the information that is actually requested by the government is not an element but merely a factor in the search analysis, and a relatively unimportant one at that, given the strong similarities between CSLI and Location History data.[159] On this view of the law, there may be a search even if the government's information request was not revealing enough to meet the intimate window threshold.[160] But of course, Judge Wynn does not concede the majority's claim that, as a matter of fact, the government's request did not satisfy the intimate

154. *See id.* I say "something close" because the majority does not clarify whether their holding is based on Chatrie's voluntarily sharing his Location History with Google *in combination* with the lack of long-term tracking, or if these two grounds of the decision are each sufficient for the holding, on their own.

155. Carpenter v. United States, 585 U.S. 296, 311 (2018) (describing the level of insight into a person's life that time-stamped data provides).

156. *See Chatrie*, 107 F.4th at 335 (explaining that when the government accesses a wealth of intimate details about a person, that constitutes a search).

157. *See id.* at 330 (finding that the information requested did not meet the intimate window threshold).

158. *See id.* at 348 (Wynn, J., dissenting) (stating that "the Court clearly considered the factors in their totality").

159. *See* United States v. Chatrie, 107 F.4th 319, 371–72 (4th Cir. 2024)

> [T]he majority opinion focuses on intimacy and voluntariness in its lengthy response to this dissent. But intimacy is only one of the factors to which the Court looked in *Carpenter*. And even if the shorter duration of the intrusion in this case leads the intimacy factor to weigh less strongly in favor of deciding that the Fourth Amendment applies, it far from tips the scale given the immense weight of the comprehensiveness (in breadth and depth), efficiency, and retrospectivity of Location History. The majority opinion does not dispute that these factors apply to Location History.

160. *See id.* at 365 (arguing that *Carpenter* created a multifactor test).

window threshold.[161] He argues that the geofence at issue *did* request enough information to create an intimate window into Chatrie's life.[162]

The fact that Judge Wynn's arguments did not carry the day is interesting in itself. It is some evidence that judges are more attracted to the element view, and some precedent for other circuits to adopt that position, though obviously not binding. But if we delve deeper into the details of the *Chatrie* split, we can identify some of the arguments for both positions and their relative merits. Ultimately, I think the majority provides a strong articulation of its interpretation of *Carpenter*. I illustrate this below in two steps, first by arguing that the majority has a better interpretation of what is required for a search under *Carpenter* and, second, that this interpretation of *Carpenter* is not satisfied in *Chatrie*, and probably not satisfied in most geofencing cases. If I'm right about these claims, then it seems that geofences generally will not be searches.

1. The Majority's Interpretation of Carpenter is Defensible and Likely to be Followed

According to the majority's view of the law, the government's information request must be sufficiently revealing for it to be a search—it must at least create an intimate window into the defendant's life.[163] The dissent denies any such requirement, holding that the revealingness of the information requested is just one factor that determines whether a search has occurred.[164] Who is right?

As I argued above, *Carpenter* makes it impossible to decisively answer this question. Footnote three in that opinion left open the majority's theory of the law as well as the

161. *See id.* at 354 (refusing to concede that the purported search was not sufficiently intimate).

162. *See id.* (arguing that the information revealed was sufficiently intimate).

163. *See id.* at 332 (majority opinion) ("The government obtained only two hours' worth of Chatrie's location information, which could not reveal the privacies of his life.").

164. *See id.* at 344 (Wynn, J., dissenting) (reasoning that the Supreme Court has laid out a multifactor approach for determining whether a search has occurred).

dissent's.[165] All *Carpenter* held was that seven days of CSLI data was a search.[166] It did not provide a clear framework for evaluating more modest requests of information.

Nevertheless, I think the majority's position exerts greater appeal for judges and is likely to be influential. One reason is that though the Supreme Court in *Carpenter* refused to *say* that there was a threshold of information collection beneath which there would be no search, it *held* that seven days of CSLI was a search, and it *reasoned* that this was partly due to the quantity of information revealed over that time span.[167]

While these three aspects of the opinion are compatible with each other, the latter two encourage lower courts to "anchor" their judgments of what constitutes a search at seven days.[168] As the amount of data acquired by the government shrinks, presiding courts will feel that they are stepping ambitiously beyond *Carpenter*. Hence, cautious courts will prefer to stick as closely as possible to the facts that *Carpenter* makes salient, even if the terms of that opinion are, officially speaking, more generous.

Further, "extrinsic" evidence for the element interpretation is that it is heavily favored by commentators and courts. Susan Freiwald and Stephen Smith have suggested that there would be "room for doubt" about whether historical CSLI tracking for shorter than seven days would be a search, precisely on the grounds that the "level of intrusiveness" would be less than in *Carpenter*.[169] Judges have also sharply distinguished expansive

---

165. *See* Carpenter v. United States, 585 U.S. 296, 310 n.3 (2018) ("It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.").

166. *See id*. (holding that the obtainment of the CSLI data for seven days was a search under the Fourth Amendment).

167. *See id.* at 312 ("[T]he suspect . . . has effectively been tailed every moment of every day for five years, and the police may—in the Government's view—call upon the results of that surveillance without regard to the . . . Fourth Amendment. Only the few without cell phones could escape this tireless and absolute surveillance.").

168. *See* Adrian Furnham & Hua Chu Boo, *A Literature Review of the Anchoring Effect*, 40 J. SOCIO. ECON. 35, 37 (2011) ("[A]nchoring bias is caused by insufficient adjustment because final judgements are assimilated toward the starting point of a judge's deliberations.").

169. *See* Freiwald & Smith, *supra* note 140, at 228, (stating that "[t]here is room for doubt" for historical CSLI for fewer than seven days "under a multifactor analysis, because the level of intrusiveness is not the same as in

and modest information acquisition by the government under *Carpenter*.[170]

The element view is not just interpretively favored. It also avoids difficult conceptual questions, such as: if the actual request from the government did not sufficiently intrude on the defendant's reasonable expectations of privacy, then *why would* such a request infringe on the Fourth Amendment? The factor view is forced to say that a search can be accomplished by the obtaining of records that *easily could have but did not*, as a matter of fact, intrude on the defendant's reasonable expectations of privacy.

Carpenter")*; see also* Ohm, *supra* note 133, at 374, ("A future court asked to rule on the warrantless access of a single datum of location information might well distinguish it from the facts and reasoning of *Carpenter*.").

170. *See In re* Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 736 (N.D. Ill. 2020) ("The far shorter time frame of government monitoring involved in the proposed geofences here raises questions about the degree to which *Carpenter* may support a conclusion that in this case, the geofences constitute a search for Fourth Amendment purposes."); Sanchez v. L.A. Dep't of Transp., CV 20-5044, 2021 WL 1220690, at *3 (C.D. Cal. Feb. 23, 2021) ("In order for [Mobility Data Specification] to be a search, the City must be able to not only de-anonymize one trip, but also identify and compile *all* the trips that Plaintiffs took on scooters . . . despite the fact that they are completely untethered from each other within the data set."); Sanchez v. L.A. Dep't of Transp., 39 F.4th 548, 560 (9th Cir. 2022) ("[I]n contrast to the CSLI at issue in *Carpenter* and the beeper tracking in *Jones*, the MDS data does not 'pervasive[ly] track' users over an extended period . . . instead capturing only the locations of e-scooters during discrete trips." (citing Carpenter v. United States, 585 U.S. 296, 314 (2018))); Commonwealth v. Perry, 184 N.E.3d 745, 762 (Mass. 2022) ("[T]he sheer volume of information investigators obtained from the tower dumps would have been impossible to gather using traditional surveillance."); *In re* Search of Info. Stored at Premises Controlled By Google, No. 22-MJ-01325, 2023 WL 2236493, at *8 (S.D. Tex. Feb. 14, 2023) ("[T]his situation is different from *Carpenter* and *Jones* because the time period involved in this warrant is much more brief: a total of 105 minutes scattered across a period of 21 days in the publicly accessible [b]usiness location."); United States v. Hay, 601 F. Supp. 3d 943, 952–53 (D. Kan. 2022), *aff'd*, 95 F.4th 1304 (10th Cir. 2024) ("[Though] the camera could record every movement Hay made within its view, the camera could not track his movements anywhere else. Unlike the GPS and CSLI technologies in *Jones* and *Carpenter*, the camera . . . revealed just a small part of that much larger whole, even if an important one."); Sims v. State, 569 S.W.3d 634, 646 (Tex. Crim. App. 2019) ("Appellant did not have a legitimate expectation of privacy in his physical movements or his location as reflected in the less than three hours of real-time CSLI records accessed by police by pinging his phone less than five times.").

The majority makes this point in the course of crisply explaining its theory of the law, writing that:

> Location History has capabilities much like GPS data and CSLI. But unlike in *Carpenter* or *Jones*, the government in this case obtained only two hours' worth of Chatrie's Location History data. Although this brief glimpse into his whereabouts may have revealed the locations he visited, it was plainly insufficient to offer insights into his habits, routines, and associations. So the government did not invade his legitimate expectation of privacy by obtaining it.[171]

In other words, the majority agrees that there are factors that govern whether the kind of data the government used is sufficiently like the CSLI data in *Carpenter*, but there is also, in its view, a further dimension to the search analysis: whether the government accessed enough data to create an appreciable risk (not just a bare possibility) of creating an intimate window into the defendant's life, by revealing his "familial, political, professional, religious, and sexual associations."[172] Again, this element has some logic behind it: if a particular geofence did not infringe on a defendant's expectations of privacy, then why should it be a search?

There may be answers. Prophylaxis is one. Perhaps some data is too tempting or too powerful, and so it is foreseeable that it will be abused or overused. Hence, as a rule or matter of policy, such requests of such data should always be considered a search. But this seems like overkill given that the nature of the geofence can be read from its terms. Any abusively large search requests can be suppressed after the fact.[173] Besides, prophylaxis has its own costs. If requesting a certain kind of data always requires a warrant even when the request would not invade a reasonable expectation of privacy, then some investigative efforts are foreclosed even though the privacy of the target is not in serious jeopardy. Why should all uses of CSLI require a warrant just because some of them will intrude on privacy?

---

171. United States v. Chatrie, 107 F.4th 319, 335–36 (4th Cir. 2024) (majority opinion).

172. *Id.* at 328.

173. *See* Mapp. v. Ohio, 367 U.S. 643, 657, 660 (1961) (finding the exclusionary rule an applicable remedy for evidence obtained in violation of the Fourteenth Amendment).

To this point I have been defending the majority, but I do not want to give the impression that its reasoning is unassailable. Given the ambiguity of *Carpenter* and the ongoing debates about how to understand its test, the Fourth Circuit opinion in *Chatrie* is better read as a strong articulation of one highly defensible approach to geofences over public areas. According to it, there is a point at which the government's request for information is so modest that there is no search.[174] Insofar as this is the law, it will be exceptional for a geofence to be a search under the Fourth Amendment.

Still, future circuit cases about geofences are more likely to be opportunities for different approaches to *Carpenter* to evolve than an occasion to mechanically apply settled precedent, and in this evolutional process, the disagreements between the *Chatrie* majority and dissent will like reappear.

2. The Geofence in *Chatrie* Is Not a Search Under the Majority's Interpretation of *Carpenter*

Now assume, as I just argued, that the majority is right about the law and that a sufficient amount of revealingness is a necessary element for the government's information gathering to constitute a search. With that assumption in mind, consider this factual question: Was the location data requested by the government's geofence enough to satisfy this element? That is to say, did it create an "intimate window" into Okello Chatrie's life?[175]

174. *See Chatrie*, 107 F.4th at 330–31 ("The government requested and obtained only two hours' worth of Chatrie's Location History data. By no means was this an all-encompassing record of [Chatrie's] whereabouts . . . . A record of a person's single, brief trip is no more revealing than his bank records or telephone call logs.").

175. *See id.* ("The government requested and obtained only two hours' worth of Chatrie's Location History data. By no means was this an 'all-encompassing record of [Chatrie's] whereabouts . . . provid[ing] an intimate window into [his] person[al] life.'" (citing Carpenter v. United States, 585 U.S. 296, 311 (2018))). Admittedly, this question is already somewhat ill-posed, since it assumes that the relevant test should be centered on Chatrie himself, when an important characteristic of geofences is that they risk revealing information about unknown others.

I think the answer is no,[176] but Judge Wynn argues at length that the answer is yes, on several grounds.[177] One of his arguments is that the geofence in *Chatrie* meets the intimate window threshold because geofences *generally* can be used to gather information from private spaces.[178] This argument is problematic. Though I agree that private spaces always, or presumptively, provide an intimate window into a person's life, this does not entail that all geofences provide such a window, for the simple reason that geofences do not necessarily cover private spaces. Some do not,[179] and why shouldn't they be judged according to the kind of space they expressly target? Why should a geofence over a non-private space be judged according to rules that are designed to address geofences over private spaces?

In response, Judge Wynn offers a kind of slippery slope argument. He argues that the constitutionality of surveillance should not be judged by what it actually reveals.[180] After all, the surveillance in *Carpenter* was a search even though it never actually intruded on any of Timothy Carpenter's private

176. *See* Wallace-Wolf, *supra* note 24, at 19–22 (arguing that *under Carpenter*, there is no intrusion by geofence searches). Further, on a correct understanding of locational privacy, I believe there was. *Id.* The law needs to be adjusted to account for this latter fact. *Id.*

177. *See Chatrie*, 107 F.4th at 348 (Wynn, J., dissenting) ("A faithful reading of *Carpenter*—not to mention common sense—compels the conclusion that when the police obtained Chatrie's Location History data, they engaged in a Fourth Amendment search. That conclusion is evident upon evaluating how the *Carpenter* factors apply to the Location History intrusion in this case.").

178. *See id.* at 351 ("It was also the case in *Carpenter* that no facts showed that the CSLI intrusion entered the defendant's own protected spaces.").

179. *See* United States v. Rhine, 652 F. Supp. 3d 38, 68 (D.D.C. 2023) ("The [Geofence Warrant] application sought . . . data . . . on January 6, 2021 for individuals in a target area slightly larger than but roughly tracing the contours of the Capitol building itself, excluding most of the plazas and lawns on both sides of the building and the abutting streets."); *see also* State v. Contreras-Sanchez, 5 N.W.3d 151, 156–57 (Minn. Ct. App. 2024) ("The geofence-warrant application sought location-history data for devices within a 65-foot-wide by 290-foot-long geofence. The proposed geofence 'encompasse[d] a public roadway and a portion of a right of way ditch.'").

180. *See Chatrie*, 107 F.4th at 353–54 ("[I]t does not matter whether the intrusion here revealed intimate information about Chatrie personally. *Carpenter* did not mention any facts that the CSLI search revealed about the defendant . . . the Court assessed only whether the search *could* reveal intimate information . . . . The search here certainly could—and did.").

spaces.[181] Likewise, the surveillance in *Kyllo* was a search even though it may not have turned up any "intimate details."[182]

But geofences are distinguishable. They need not even *risk* intruding on a private location. It is true that once one starts tracking an individual person's movement (e.g., Timothy Carpenter's), historically or in real time, one cannot predict whether they and hence one's surveillance, will enter private space. That risk is inherent in one's tracking. The same is true of thermal imaging technology aimed at a house. One has no guarantee that one will not thereby learn something intimate. But the coverage of a geofence is specified beforehand and does not change as those inside them move.[183] Hence, it seems that there is no slippery slope from geofencing in general to geofencing a private area. Instead, there is a policeable, administrable distinction between geofences that cover private areas and those that do not. And the fact that the former would meet the intimate window threshold should not mean that the latter meets it as well. The standard for geofences should vary depending on what they cover, and so appealing to the intimacy of private spaces should not be sufficient to show that a geofence over a public space is a search.

A second argument put forward by Judge Wynn is that the geofence in this case *was* placed over a private space, given that it may have captured information from the nearby apartment complex.[184] This is an argument that deserves greater consideration, because geofences, unlike the tracking of a

181. *See* Carpenter v. United States, 585 U.S. 296, 310 (2018) ("A person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, 'what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.'" (quoting United States v. Katz, 389 U.S. 347, 351–52 (1967))).

182. *See* Kyllo v. United States, 533 U.S. 27, 28 (2001) ("Also rejected is the Government's contention that the thermal imaging was constitutional because it did not detect 'intimate details.' Such an approach would be wrong in principle because, in the sanctity of the home, *all* details are intimate details.").

183. *See* United States v. Chatrie, 107 F.4th 319, 324 (4th Cir. 2024) (majority opinion) (describing the geofence warrant process).

184. *See id.* at 355 (Wynn, J., dissenting) ("The geofence intrusion here was so broad that it could have followed users through dozens of non-public spaces, including residences, religious spaces, and senior living facilities. Thus, the intrusion did not merely constitute a short-term tracking of public movements." (internal quotation omitted)).

particular person's movements, are by their nature "wide."[185] They are liable to reveal location information about nearby citizens that are unrelated to the government's investigation.[186] This concern is heightened when nearby citizens are at home. How should this aspect of geofences figure into the analysis of whether they are a search?

Unfortunately, the majority does not give this question the fresh consideration it deserves. Instead, it cites the ordinary rule, which is that a defendant cannot challenge intrusions into private spaces that are not his own.[187] According to this rule, the fact that the geofence revealed information from the private spaces of other people is irrelevant to whether it was a search of Chatrie himself, or whether it was a search that he can challenge.

Though I doubt that this traditional rule is appropriate given the nature of geofences, the majority does not point out two other considerations that provide some support for its holding. One is that the geofence initially anonymizes those who are caught within it.[188] Perhaps third-parties who are revealed to be located at a particular residence can be identified (by information about who lives at the residence), but this need not always be true. Someone in a residence does not necessarily live there and other private spaces may not provide a ready way to identify those found within them. Hence, the anonymity of geofencing may somewhat ameliorate its privacy consequences

185. *See* United States v. Chatrie, 590 F. Supp. 3d 901, 926 (E.D. Va. 2022) (noting that geofences do not fit into Supreme Court precedent because they are wide but not deep).

186. *See id.* at 930 (highlighting the data collected from beyond the bank area).

187. *See Chatrie*, 107 F.4th at 336–37 (majority opinion) ("Chatrie does not allege that the Location History data obtained by the government invaded his constitutionally protected space, like his home. And to the extent that it may have showed him or others in *someone else's* protected space, Chatrie lacks standing to assert that person's potential Fourth Amendment rights.") (emphasis in original). *See also* United States v. Davis, 109 F.4th 1320, 1328–39 (11th Cir. 2024) (holding that defendant could not challenge the tracking of his companion's phone, despite the fact that such tracking revealed his location as a consequence).

188. *See Chatrie*, 107 F.4th at 324 ("Google's procedure works as follows: At Step One, law enforcement obtains a warrant that compels Google to disclose an anonymous list of users whose Location History shows they were within the geofence during a specified timeframe.").

for those caught within it, though perhaps not decisively. The second point is that the geofence in *Chatrie* did not cover private space, by its terms. Given the margin of error for Google location data, it *risked* revealing information from well beyond its parameters (i.e., the residences),[189] but this is different than placing the geofence over a private area. Again, I do not claim that this difference decisively supports the government's geofence in this case, but it is an important distinction.

Judge Wynn does not meet the majority's invocation of the ordinary "third-party standing" search rule with a different one; one more suitable for searches that are "wide" and thus predictably or likely reveal information about others. Instead, he relies on the arguments I enumerated earlier, according to which the geofence as it applied to Chatrie should be judged by the capabilities of geofencing generally.[190] I argued above why I do not think that is correct.[191]

Let me make one final point about the *Chatrie* geofence's inclusion of nearby residences, to keep the focus on my main point. Geofences need not cover private spaces,[192] and it is plausible that special rules should govern those that do, or might, given margins for error in location data. If this is correct, then *Chatrie* is, arguably, not correctly decided. But while significant for this case, it is not a detail that should distract from my main line of argument. The government in *Chatrie could have*, at little to no investigative cost, altered the geofence to exclude information from any residences.[193] And if it did, then the geofence would have only captured two hours of location data about people in public places. The question would then be whether *that* data would meet the intimate window threshold. This question goes to the core of geofencing surveillance, and it cannot be answered by invoking the intimacy of private spaces.

Judge Wynn also answers this harder, more fundamental question, affirmatively. He argues that:

---

189. *Chatrie*, 107 F.4th at 350 (Wynn, J., dissenting).

190. *See supra* Part II.B.2.

191. *See supra* Part II.B.2.

192. *See Chatrie*, 107 F.4th at 324 (majority opinion) (noting that police decide the area of the geofence).

193. United States v. Chatrie, 107 F.4th 319, 324 (4th Cir. 2024).

> [T]he geofence intrusion occurred in a busy part of the Richmond metro area between 3:50 and 5:50pm. That is when most people leave work or school and travel to their next destinations, carrying their phones into intimate spaces and engagements. A two-hour search could tour a person's home, capture their romantic rendezvous, accompany them to any number of medical appointments, political meetings, strikes, or social engagements . . . .[194]

In other words, he argues that the threshold required to satisfy the "intimate window" threshold could be as low as two hours.

But this is a bold claim—not even Carpenter himself argued that there would be a search when the government acquired information about someone for less than a day.[195] The intimate window bar is not that low. After all, just about any information *might* reveal something intimate about someone. One might see someone entering an abortion clinic during a half second glance in their direction, but one is permitted to glance and does not violate privacy by doing so. In other words, whatever non-trivial threshold level of revealingness is required to create an intimate window into someone's life, geofences will plausibly fall below it.

As *Carpenter* puts it, information about a person's movements through public space does not provide an intimate window into someone's life when it reveals "only his particular movements," but only when those movements can be reasonably *expected* to reveal, or *characteristically* reveals information about their "familial, political, professional, religious, and sexual associations."[196]

The majority is thus on good ground when it invokes *Beautiful Struggle's* holding that *Carpenter's* "intimate window" language should be understood in terms of the mosaic theory.[197] According to this theory, the revealingness of relatively

---

194. *See Chatrie*, 107 F.4th at 353 (Wynn, J., dissenting).

195. *See* Carpenter v. United States, 585 U.S. 296, 310 n.3 (2018) ("The parties suggest as an alternative to their primary submissions that the acquisition of CSLI becomes a search only if it extends beyond a limited period.").

196. *See id.* at 311.

197. *See Chatrie*, 107 F.4th at 353 ("Although not couched under this label, *Beautiful Struggle* articulated a version of what one scholar calls the "Mosaic Theory" of the Fourth Amendment." (citing Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 336 (4th Cir. 2021))).

unconnected information about a person should be distinguished from the greater kind of exposure that is achieved when various data points can reinforce and contextualize each other, so that a picture of what the person does "ensemble" emerges.[198] Moreover, lower courts that have applied *Carpenter* routinely characterize it as embracing the mosaic theory,[199] and they also understand that theory as distinguishing between the minimal revealingness of isolated trips through public space, and the more concerning exposure that stems from a wider collection of such trips.[200] The latter is what tends to reveal a person's First Amendment associations.

In response, Judge Wynn repurposes his earlier point about how *Carpenter* found a search despite not identifying any intimate detail that the CSLI tracking revealed. He writes that "*Carpenter* did not mention any facts that the CLSI search revealed about the defendant in that case—rather, the Court assessed only whether the search *could* reveal intimate information unrelated to legitimate police needs."[201]

True enough. *Carpenter* did not identify any actual intimate details that were revealed about Timothy Carpenter, but, the absence of such details does not entail that the bare possibility of revealing intimate information meets the intimate window threshold. Again, *Carpenter* can plausibly be read as requiring the collection of information that characteristically reveals intimate information, such as information about a private space, or a sufficiently large amount of information about one's public comings and goings.

I conclude that the majority is correct in arguing that tracking a person's public movements for two hours is not sufficiently likely to reveal their First Amendment associations, and so does not create an "intimate window" into their life generally, even if there is, as there always is, a bare possibility that it would reveal something intimate.

---

198. Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 342 (4th Cir. 2021).

199. *See, e.g.*, United States v. Tuggle, 4 F.4th 505, 517 (7th Cir. 2021) ("Some judges and justices have relied on mosaic-like reasoning, but the Supreme Court has not bound lower courts to apply the mosaic theory.").

200. *Id.* at 518.

201. *Chatrie*, 107 F.4th at 354.

3. The Overall Lesson: Geofences Evade Current Search Doctrine

With the foregoing discussion, I have supported the claim that geofencing evades current Fourth Amendment search doctrine. The argument to that effect can be summarized as follows. Under one viable and attractive interpretation of current law, the actual revealingness of the government's information request has a special significance compared to the potential revealingness of the kind of records it queries. If the request is not actually very revealing, then this is a factor of great weight or even decisive in supporting the conclusion that it is not a search. After all, the government has not acted in a way that presents any more than a bare possibility of intruding on the Fourth Amendment touchstone: the defendant's reasonable expectations of privacy.

If this proposition of law is granted, then geofences will not generally be searches, since their defining characteristic is that they are wide but shallow, and so do not acquire much information about those that they ensnare. Thus, the average defendant seeking to suppress the results of a geofence that includes them in it will not succeed, on the grounds that their privacy was not sufficiently put in jeopardy.

C. *Objection:* United States v. Smith

Just weeks after *Chatrie*, the Fifth Circuit issued *United States v. Smith*.[202] The opinion is significant for three reasons. First, its consideration of geofencing *warrants* is radical and controversial.[203] Second, it rejects *Chatrie's* formalistic reasoning about the voluntariness of turning on Location History.[204] Third, it rejects *Chatrie's* reasoning with regard to

202. 110 F.4th 817 (5th Cir. 2024).

203. *See* Orin S. Kerr, *The Fifth Circuit Shuts Down Geofence Warrants—And Maybe A Lot More*, REASON: THE VOLOKH CONSPIRACY (Aug. 13, 2024), https://perma.cc/548W-CVUV ("[T]he Fifth Circuit's ruling, although announced in a case that happens to be about geofence warrants, is about . . . . pretty much all database queries. . . . Just create a data source big enough—how big, we don't know, but big—and then it can't be searched, even with a warrant.").

204. *See Smith*, 110 F.4th at 834 ("[W]hile cell phone data is held by private corporations, on a practical level, it is unreasonable to think of cell

whether geofencing violates a reasonable expectation of privacy.[205] I will focus on the third claim. Is *Smith* right to reject *Chatrie's* privacy analysis? Does it show that *Chatrie's* reasoning on that issue is unconvincing after all, despite my arguments above?

I do not think so. The Fifth Circuit's opinion is highly focused on Location History data as a kind of record. Indeed, it correctly notices that there are several important and concerning "parallels between CSLI and Location History data."[206] However, it does not ask the question whether such a parallel is legally decisive under *Carpenter*. Instead, it simply assumes as much, glossing over the record/revealingness distinction, as well as the *Chatrie* majority's insistence that there is more to *Carpenter's* test than just whether a record-type is sufficiently like CSLI.[207] Its failure to engage the *Chatrie* opinion's legal theory is a serious shortcoming.

The closest the *Smith* court comes to touching the *Chatrie* majority's reasoning is in its attempt to respond to its admission that "geofences tend to be limited temporally."[208] The court's twofold response however shares the weaknesses of some of Judge Wynn's arguments.

The *Smith* court argues first that the "potential intrusiveness of even a snapshot of precise location data should

---

phone users as voluntarily assuming the risk of turning over comprehensive dossiers of their physical movements to third parties.").

205. *See id.* at 833 ("Characterizing Location History data as nothing more than a 'record of a person's single, brief trip,' the Fourth Circuit found that geofencing does not contravene a person's 'reasonable expectation of privacy' . . . . With great respect to our colleagues on the Fourth Circuit, we disagree.").

206. *See id.* at 836 ("Given the intrusiveness and ubiquity of Location History data, Smith and McThunel correctly contend that they have a reasonable expectation of privacy in their respective data.").

207. *See* United States v. Chatrie, 107 F.4th 319, 335–36 (4th Cir. 2024) (majority opinion)

> Location History has capabilities much like GPS data and CSLI. But unlike in Carpenter or Jones, the government in this case obtained only two hours' worth of Chatrie's Location History data. Although this brief glimpse into his whereabouts may have revealed the locations he visited, it was plainly insufficient to offer insight into his habits, routines, and associations. So the government did not invade his "legitimate 'expectation of privacy' by obtaining it.

208. *Smith*, 110 F.4th at 833.

not be understated"[209] since "even a brief snapshot can expose highly sensitive information."[210]

But the key word is "can." It is true that a brief snapshot can—in the sense of "there is a bare possibility"—expose sensitive information, but this is too low of a bar. Almost any surveillance of a person carries some risk of revealing intimate information about a person. But this risk does not entail that a reasonable expectation of privacy has been invaded. *Carpenter* requires revealing enough location information such that one would characteristically learn something about their "familial, political, professional, religious, and sexual associations."[211]

The *Smith* court argues, second, that "location tracking can easily follow an individual into areas normally considered some of the most private and intimate."[212] But we saw the problem with this argument before. The fact that geofencing could be abused does not entail that any particular geofence was. The geofence in this case arguably did not cover any private areas and it certainly did not cover any of *Chatrie's* private spaces.[213] In any case, this argument will not work against geofences placed over thoroughly non-private spaces.

Again, I think the Fifth Circuit is, like Judge Wynn, right to be concerned about geofencing, but I do not think that current doctrine invests their concerns with as much legal heft as they think.

CONCLUSION

Concern about the Fourth Amendment status of geofencing has been brewing for years, first among magistrate judges and then among state and federal trial judges. They have wondered whether geofencing surveillance is a search, and they have worried that it is not.

---

209. *Id.*

210. *Id.* (quoting Haley Amster & Brett Diehl, *Against Geofences*, 74 STAN. L. REV. 385, 408 (2022)).

211. Carpenter v. United States, 585 U.S. 296, 311 (2018).

212. United States v. Smith, 110 F.4th 817, 833 (5th Cir. 2024).

213. *See id.* at 826 ("[A]s with any geofence warrant, no specific Google accounts were identified in Section I of Attachment A; rather, the Attachment only specified specific coordinates around the Lake Cormorant Post Office.").

The Fourth Circuit in *United States v. Chatrie* has provided the first appellate confirmation of these worries, holding that the geofence at issue did not implicate the defendant's reasonable expectations of privacy. In so holding, it relied on the third-party doctrine. However, the opinion provides plenty of argumentation that supports an alternative rationale, according to which geofencing is not generally a search under *Carpenter*, just in virtue of the fact that it does not open an intimate window into the lives of those caught in it. This view is likely to be challenged in coming years as the digital Fourth Amendment comes even more clearly into view, but until that time, the dissent is correct in lamenting that, in the Fourth Circuit at least, "the government is permitted to retroactively surveil American citizens anywhere they go—no warrant needed—so long as it keeps it snooping to a few hours . . . ."[214]

214. *Chatrie*, 107 F.4th at 335–36 (Wynn, J., dissenting).