YALE LAW & POLICY REVIEW

Find My Friends, Lose My Privacy? Responding to Third-Party Doctrine's Failure in the Digital Age

*Nicole Alexandra Plante**

This Note examines the application of third-party doctrine to location data and argues that the doctrine, as it currently stands, is unworkable in the modern digital era. Third-party doctrine holds that individuals forfeit Fourth Amendment protections when they voluntarily and knowingly share information with third parties, such as map or social media applications. However, individuals today routinely share sensitive location data with third parties, often without full awareness or meaningful consent. The Supreme Court acknowledged this challenge in Carpenter v. United States*, carving out an exception for location information collected by cell towers, but failing to provide a clear framework for lower courts to apply.*

This lack of guidance resulted in a circuit split between the Fourth and Fifth Circuits, each interpreting Carpenter *to reach opposite conclusions on whether location data is voluntarily shared, followed by the Fourth Circuit subsequently rehearing the case and not reaching a majority on* Carpenter *and third-party doctrine. This circuit split, and subsequent indecision, highlights the challenge in applying third-party doctrine to location data and underscores the need for a new approach.*

To resolve this issue, this Note proposes the Purpose-Sensitivity approach, a test that hinges Fourth Amendment protections on (1) whether the individual's purpose in sharing their location data was to broadly share it with

* Yale Law School, J.D. expected 2026. I am deeply indebted to Professor Tracey Meares for cultivating my interest in criminal procedure and guiding me along the way. Without her guidance, thought-provoking questions, and support this Note would never have materialized. I want to thank Raymond Perez, Artha Jonassaint, Drew Jones, Priscilla Samey, and all the editors of Yale Law & Policy Review for their hard work and feedback during this process. To my family, thank you for your constant support throughout law school. And finally, thank you to Chase Hinman for your encouragement and insight. All views, errors, and omissions are my own.

the public, and (2) whether the location data does or could contain sensitive information. This approach is both informed by the circuit courts' reasoning and in line with Fourth Amendment jurisprudence, ensuring a more consistent and constitutionally sound application of third-party doctrine to location data. By refining the doctrine, this Note offers a solution that better balances individual privacy rights with law enforcement's interests in the digital age.

INTRODUCTION

How many third parties are you sharing your location data with? First to come to mind might be Apple through Find My or Google through Google Maps, or maybe even Uber. If you open your phone and go to location services, chances are there are dozens of apps actively logging your location information. Many of these apps have no apparent reason to be constantly tracking you. Even if you have your apps' location services set to "while using," these apps may be able to track your location while running in the background.[1] Not only can the companies operating these apps see your location, the government too can access all of that data[2] without infringing on your Fourth Amendment rights because of a judge-made rule called third-party doctrine. Under third-party doctrine, when you check your weather app every morning and it pings your location, the government can see that. Or when you use the Find My Friends app to share your location with friends and family, the government can see that. Even when you allow Yelp to find restaurants near you, play games like PokemonGo, or order an Uber, that location data is freely accessible to the government under this doctrine. It may seem surprising that the government can ubiquitously search your location data, but if you have shared it with a third party (Apple, Google, Yelp, etc.), then according to third-party doctrine, you lose your Fourth Amendment rights.

Third-party doctrine holds that if a person "knowingly and voluntarily" shares information with a third party, then they no longer have a reasonable expectation of privacy in that information and thus no Fourth Amendment protections. This doctrine was born out of two cases in the late 1970s—*United States v. Miller* and *Smith v. Maryland*—which gave the government access to bank records and phone numbers consistent with the Fourth Amendment on the basis that the users shared this information with the

1. *About Privacy and Location Services in iOS, iPadOS, and watchOS*, APPLE, https://support.apple.com/en-us/102515 [https://perma.cc/683V-R4YY] ("An app is considered 'in use' . . . when it is using location in the background . . . .").

2. By data, this Note is referring to the location information that applications collect and store.

bank and phone company.[3] However, the world looks different today: It is necessary to share our most intimate details with third parties,[4] including location information.[5] As Justice Sotomayor explained, "People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers."[6] Fourth Amendment precedent lags behind the times and fails to provide adequate protection.

Typically, if the police want to conduct a search they must obtain a search warrant from a judge, which requires probable cause or a fair probability that a search will lead to evidence of a crime being discovered.[7] However, under third-party doctrine, a search warrant is not required to obtain location data that has been shared with a third party. In some instances, this means police do not have Fourth Amendment–guided judicial oversight for their actions. For example, when seeking geofence data, which is a kind of location data collected from devices within a specific geographic area,[8] police must obtain initial approval from a magistrate judge to compel

3. United States v. Miller, 425 U.S. 435, 443 (1976) ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." (citing United States v. White, 401 U.S. 745, 751-52 (1971))); Smith v. Maryland, 442 U.S. 735, 743-44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

4. *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (recognizing that "in the digital age . . . people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks").

5. Many apps require location information to work or assert they need location data to work optimally. Sidney Fussell, *The Most Important Things to Know About Apps That Track Your Location*, TIME (Sept. 1, 2022), https://time.com/6209991/apps-collecting-personal-data/ [https://perma.cc/MK66-VXDY] ("Many apps on your smartphone keep track of where you are, often for obvious-sounding reasons. . . . As many as 200 million mobile devices report location data to smartphone apps . . . some logging a user's location as many as 14,000 times in a single day.").

6. *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring).

7. JAMES A. ADAMS & DANIEL D. BLINKA, PROSECUTOR'S MANUAL FOR ARREST, SEARCH AND SEIZURE § 3-2(c) (2004); Illinois v. Gates, 462 U.S. 213, 238-39 (1983).

8. A geofence warrant is a request from law enforcement to a company to give them the location history data of every device within a certain geographic

companies to provide the data. However, this process does not require probable cause or particularity, which the Fourth Amendment requires.[9] This process does not have legal origins. Instead, it was created by Google and became the standard for other companies.[10] This means that there is no law requiring police to get judicial approval: It is only required because Google decided not to provide the information without it. In essence, even when there is some form of judicial oversight, it is only at the behest of private companies, and it is not even close to a substitute for Fourth Amendment protections.[11] Additionally, many have raised concerns about how often and how quickly these requests are approved,[12] and scholars

boundary and time frame. Law enforcement then uses this data to find or narrow down users and receive their identifying information. *See, e.g.*, United States v. Chatrie, 590 F. Supp. 3d 901, 914 (E.D. Va. 2022) ("When law enforcement seeks a geofence warrant from Google, it (1) identifies a geographic area (also known as the 'geofence,' often a circle with a specified radius), (2) identifies a certain span of time, and (3) requests Location History data for all users who were within that area during that time."), *aff'd*, 107 F.4th 319 (4th Cir. 2024), *and aff'd on reh'g en banc*, 136 F.4th 100 (4th Cir. 2025) (per curiam), *cert. granted*, No. 25-112, 2026 U.S. LEXIS 705 (U.S. Jan. 16, 2026).

9. Nathaniel Sobel, *Do Geofence Warrants Violate the Fourth Amendment?*, LAWFARE (Feb. 24, 2020), https://www.lawfaremedia.org/article/do-geofence-warrants-violate-fourth-amendment [https://perma.cc/7TZF-LBNM]; Jackie O'Neil, *Much Ado About Geofence Warrants*, HARV. L. REV. BLOG (2025).

10. Orin Kerr, *The Fourth Amendment and Geofence Warrants: A Critical Look at United States v. Chatrie*, LAWFARE (Mar. 12, 2022), https://www.lawfaremedia.org/article/fourth-amendment-and-geofence-warrants-critical-look-united-states-v-chatrie [https://perma.cc/G2J2-TSTU] ("Google's process has effectively become the current way geofence warrants are carried out.").

11. This is not a sufficient replacement for the Fourth Amendment because it does not require the same protections as the Amendment. Notably, probable cause and particularity are not required. *See id.* (describing how "Google has . . . specified a three-step process that it requires investigators to follow to try to protect the privacy of Google users" that does not include probable cause and particularity requirements).

12. Jessica Miller Schreifels & Aubrey Wieber, *Warrants Approved in Just Minutes: Are Utah Judges Really Reading Them Before Signing Off?*, SALT LAKE TRIB. (Jan. 16, 2018, 10:13 AM), https://www.sltrib.com/news/2018/01/14/warrants-approved-in-just-minutes-are-utah-judges-really-reading-them-before-signing-off/ [https://perma.cc/6QYS-Y52R].

have noted that magistrate judges "often approve geofence warrants despite their flaws."[13] Under the current system, third-party doctrine allows police to avoid judicial oversight and circumvent the Fourth Amendment when searching location data. Location data, the focus of this Note, refers to all kinds of location information the government can search from a wide-ranging number of companies who track their customers.

The Supreme Court recognized the problem with applying third-party doctrine to location data in 2018, but it has yet to provide a clear solution. Instead, in *Carpenter v. United States*,[14] the Court created an exception and declined to extend third-party doctrine specifically to location information collected when cell phones connect to networks and towers, known as cell site location information (CSLI).[15] The Court noted that it was unclear if a user truly "knowingly and voluntarily" shared their CSLI with a third party[16] and commented on the difficulty in applying this logic to technology and data broadly.[17] Yet, the Court failed to provide a clean solution, instead creating an exception to the doctrine for CSLI,[18] but leaving it apparently entirely intact in all other instances[19]—including for modern-day location data. As a result, lower courts have been left with an unclear doctrine and little guidance for applying it to increasingly commonplace location tracking by third parties.

---

13. Shelby Stender, *Circumventing the Fourth Amendment: The Unconstitutional Nature of Geofence Warrants*, 2024 UTAH L. REV. 733, 737.

14. 585 U.S. 296 (2018).

15. CSLI provides a record of where a cell phone has been based on the cell phone towers and networks it interacts with. This is different from location data collected by apps that this Note in large part focuses on. Lars Daniel, *How Digital Forensic Experts Know Where You've Been—Cell Site Location Information*, FORBES (Dec. 18, 2024), https://www.forbes.com/sites/larsdaniel/2024/12/18/how-digital-forensics-experts-know-where-youve-been-cell-site-location-information/.

16. *Carpenter*, 585 U.S. at 315.

17. The Court said that "[a]fter all, when Smith was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements." *Id.* at 309.

18. For an explanation of the difference between CSLI and location data, *see infra* note 23.

19. The Court remarked that its decision was a narrow one and that it did "not express a view on matters not before [it]." *Carpenter*, 585 U.S. at 316.

In the cracks left by *Carpenter*, a circuit split grew between the Fifth and Fourth Circuits. This split shows not only that third-party doctrine is unworkable for location data and the technological era, but also how the Court's ruling in *Carpenter* is confusing for lower courts. Specifically, the initial decisions by the circuits applied *Carpenter* in conflicting ways, citing different tests and factors from the opinion to determine if third-party doctrine applied.[20] The courts came to opposite conclusions about whether geofence data, which is location data collected from devices within a specific geographic area,[21] was "knowingly and voluntarily" exposed to third parties.[22] The courts specifically struggled to determine if the exception for CSLI created by *Carpenter* could be extended further to geofence data. The difference between CSLI and location data generally is that CSLI only collects location information when a cell phone pings a tower or network, whereas location data is collected continuously through applications that track location.[23] Reading the two circuit decisions side by side highlights the challenge of making sense of third-party doctrine and the current jurisprudential guidance for using the doctrine. Subsequently, the Fourth Circuit reheard its case en banc and, due to an apparent inability to determine how to apply *Carpenter* and whether third-party doctrine applied, affirmed the lower court per curiam with eight concurrences and one dissent, all reaching different conclusions.[24] In an attempt to remedy this mess, this Note provides a new approach for courts. This new approach is intended to apply not just to geofence data, but to location data generally,[25] therefore clearing up the confusion left by *Carpenter*.

While this Note focuses on the Fifth and Fourth Circuit cases, these courts are not alone in trying to discern how third-party doctrine applies to

20. United States v. Chatrie, 107 F.4th 319, 330-32 (4th Cir. 2024), *aff'd on reh'g en banc*, 136 F.4th 100 (4th Cir. 2025) (per curiam), *cert. granted*, No. 25-112, 2026 U.S. LEXIS 705 (U.S. Jan. 16, 2026).).

21. *See supra* note 8.

22. *Chatrie*, 107 F.4th at 322; *Smith*, 110 F.4th at 820.

23. CSLI and location data differ because CSLI only tracks when a phone connects to a cell phone tower, whereas location data is collected by applications that are constantly tracking users creating "pinpoint locations." The Fifth Circuit discussed the difference, noting that "this technology provides more precise location data than either CSLI or GPS." *Smith*, 110 F.4th at 833.

24. United States v. Chatrie, 136 F.4th 100 (4th Cir. 2025) (en banc) (per curiam), *cert. granted*, No. 25-112, 2026 U.S. LEXIS 705 (U.S. Jan. 16, 2026).

25. Location data refers to all kinds of location information that applications collect and store.

location data, and in reaching different holdings. The Eleventh Circuit heard an appeal in 2024 on this topic, but it avoided the issue on other grounds.[26] The D.C. Circuit would have heard a case to address the application of third-party doctrine to geofence warrants, but President Trump's pardon of January 6 defendants mooted the case.[27] This is also an issue in state courts. The Minnesota Supreme Court is currently considering a case dealing with geofence warrants and location data.[28] The Colorado Supreme Court weighed in on the issue of location data and put out a ruling that diverges from the Fifth Circuit's conclusions.[29] Lastly, in March 2025, the Georgia Supreme Court ruled on the issue of cell phone location data and diverged from the Fifth Circuit.[30] These cases, and their differences, show the increasing need for the solution and clarity this Note provides.

The striking number of cases on the issue of geofence warrants and location data is a direct result of ever-increasing use of location data by police.[31] Indeed, Google alone "observed over a 1,500% increase in the number of geofence requests it received in 2018 compared to 2017," and

26. The judges determined that, because the appellant's case actually involved his girlfriend's phone, not his own, he could not assert a Fourth Amendment right. However, a petition for a writ of certiorari is pending before the Supreme Court that raises the question of geofence warrants and third-party doctrine. United States v. Davis, 109 F.4th 1320, 1327 (11th Cir. 2024), *petition for cert. filed*, No. 25-5189 (U.S. July 15, 2025).

27. United States v. Rhine, No. 23-3168, 2025 WL 415120 (D.C. Cir. Feb. 3, 2025). For the lower-court decision related to third-party doctrine, see United States v. Rhine, 652 F. Supp. 3d 38 (D.D.C. 2023).

28. State v. Contreras-Sanchez, 5 N.W.3d 151 (Minn. Ct. App. 2024), *reh'g granted*, No. A22-1579, 2024 Minn. LEXIS 280 (Minn. May 29, 2024).

29. People v. Seymour, 536 P.3d 1260 (Colo. 2023); *Fifth Circuit Rules that Geofence Warrants Are Inherently Unconstitutional*, ELEC. PRIV. INFO. CTR. (Aug. 13, 2024), https://epic.org/fifth-circuit-rules-that-geofence-warrants-are-inherently-unconstitutional/ [https://perma.cc/Q2DM-CLZL].

30. Jones v. State, 913 S.E.2d 700 (Ga. 2025).

31. *Supplemental Information on Geofence Warrants in the United States*, GOOGLE (Apr. 28, 2023) https://www.documentcloud.org/documents/23792109-supplemental_information_geofence_warrants_united_states/ [https://perma.cc/HXC2-6KVF]; Ilica Mahajan, *The High-Tech Tools Police Can Use to Surveil Protesters*, MARSHALL PROJ. (Nov. 12, 2024), https://www.themarshallproject.org/2024/11/12/protest-surveillance-technologies/ [https://perma.cc/5UHL-C34S].

"[i]n 2019, Google received 'around 9,000 total geofence requests.'"[32] Further, the government is using location data in ways that infringes on large groups of people's rights and avoids judicial oversight. Some may argue that it does not matter if the government can have anyone's location data because they only use it to find lawbreakers or those suspected of a crime. But when the government gains the power to deny constitutional rights to one group of people, it puts everyone's rights at risk, and, in searching location data, police search large swaths of data. This means that searching location data creates a digital dragnet, catching those suspected of a crime and those not.[33] On several occasions, location data has even led police to make false arrests.[34] Because of third-party doctrine, there is no judicial oversight and no guarantee of Fourth Amendment protection for location data.

There is much at stake when the government has access to our location data without Fourth Amendment restrictions. In this particular moment, when officials in the United States have threatened to lock up political enemies,[35] privacy rights are shrinking,[36] and states have vastly different

32. United States v. Chatrie, 590 F. Supp. 3d 901, 914 (E.D. Va. 2022), *aff'd*, 107 F.4th 319 (4th Cir. 2024), *and aff'd on reh'g en banc*, 136 F.4th 100 (4th Cir. 2025) (per curiam), *cert. granted*, No. 25-112, 2026 U.S. LEXIS 705 (U.S. Jan. 16, 2026).

33. Shira Ovide, *Police Love Google's Surveillance Data. Here's How To Protect Yourself*, WASH. POST (Oct. 24, 2023), https://www.washingtonpost.com/technology/2023/10/24/google-privacy-police-geofence/.

34. Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html/; Julia Love & Davey Alba, *Google User Data Has Become a Favorite Police Shortcut*, BLOOMBERG (Sept. 29, 2023), https://www.bloomberg.com/news/features/2023-09-28/google-user-data-is-police-s-top-shortcut-for-solving-crimes/; Johana Bhuiyan, *TechScape: How Police Use Location and Search Data to Find Suspects – and Not Always the Right Ones*, GUARDIAN (Oct. 3, 2023), https://www.theguardian.com/technology/2023/oct/03/techscape-geofence-warrants [https://perma.cc/4395-A8V8].

35. Lisa Lerer & Michael Gold, *Trump Escalates Threats to Political Opponents He Deems the 'Enemy*,' N.Y. TIMES (Nov. 8, 2024), https://www.nytimes.com/2024/10/15/us/politics/trump-opponents-enemy-within.html.

36. Maurizio Guerrero, *The Growing Surveillance State in the U.S. Is Far Worse Than You Imagined*, PRISM REPS. (July 10, 2025), https://prismreports.org/2025/07/10/surveillance-state-in-u-s-is-far-worse-than-you-imagined/ [https://perma.cc/4J39-8S9L].

guaranteed rights, these concerns are more pressing than ever. For example, if the government can track someone to a doctor's office, can they then use that information in determining the cost of their Medicare? Or if the government tracks someone leaving Texas to go to an abortion clinic in a nearby state, can Texas use that information to prosecute them? What about protests? Can the government get the location information of anyone at a protest and use it to limit their First Amendment right to protest, or as justification to deport them?[37] And these situations are not just hypothetical. The government has already used location information to "infer people's immigration status, religion, and sexual orientation,"[38] and track large swaths of innocent civilians to monitor single targets.[39] Police have been increasingly using location data to target protesters, raising not only Fourth Amendment but also First Amendment concerns.[40] For example, the police used location data to track protestors during the Black Lives Matter protests,[41] and to track protestors on college campuses.[42] The police in Idaho, where abortion is illegal, also used cell phone location data in an investigation to track a woman leaving the state to obtain an

37. Mike Fong, *Going to a Protest? Keep Your Smartphone from Being Used as a Tracking Device*, FORBES (Aug. 21, 2020), https://www.forbes.com/councils/forbestechcouncil/2020/08/21/going-to-a-protest-keep-your-smartphone-from-being-used-as-a-tracking-device/.

38. Sidney Fussell, *The Most Important Things to Know About Apps That Track Your Location*, TIME (Sept. 1, 2022), https://time.com/6209991/apps-collecting-personal-data/ [https://perma.cc/46BX-VBXV].

39. As the Fifth Circuit explained, "Of particular concern is the fact that a geofence will retroactively track anyone with Location History enabled, regardless of whether a particular individual is suspicious or moving within an area that is typically granted Fourth Amendment protection." United States v. Smith, 110 F.4th 817, 834 (2024), *cert. denied*, No. 24-7237, 2025 U.S. LEXIS 4192 (U.S. Nov. 10, 2025).

40. Ari Sen, *UNC Campus Police Used Geofencing Tech to Monitor Antiracism Protestors*, NBC NEWS (Dec. 21, 2019), https://www.nbcnews.com/news/education/unc-campus-police-used-geofencing-tech-monitor-antiracism-protestors-n1105746 [https://perma.cc/BAH4-SN54]; *see also* Mahajan, *supra* note 31.

41. *See, e.g.*, Zak Doffman, *Black Lives Matter: U.S. Protestors Tracked by Secretive Phone Location Data*, FORBES (June 26, 2020), https://www.forbes.com/sites/zakdoffman/2020/06/26/secretive-phone-tracking-company-publishes-location-data-on-black-lives-matter-protesters/.

42. *See, e.g.*, Sen, *supra* note 40.

abortion.[43] Under third-party doctrine, a vast majority of this location data likely evades Fourth Amendment protection.

This Note aims to help courts understand how to extend third-party doctrine to location data through a new test that marries recent case law with the original intent and text of the Fourth Amendment. This Note's test focuses solely on location data because third-party doctrine has proven specifically unworkable for location data, as evidenced by *Carpenter* and the circuit split. This new test, the Purpose-Sensitivity approach, focuses on the individual's purpose in sharing their data and their demonstrated sensitivity interests. It asks two questions: (1) in sharing their location data with third parties, was the user's purpose to share that information broadly with the public?; and (2) does or could the location data shared contain sensitive information? Within each of these prongs, this Note proposes a number of factors for courts to consider, which draw from existing precedent. Not only is this test grounded in the circuit courts' decisions, but it is also aligned with Fourth Amendment jurisprudence and the original intent and text of the Fourth Amendment, making it highly feasible.

Scholars have long recognized the problems with and dangers of third-party doctrine.[44] Previous proposals, however, fail in the digital age and in light of the circuit court decisions. This is because most rely heavily on the "knowingly and voluntarily exposed" test, looking at consent and contracts, but the circuit courts show that this test is unworkable in the digital age. Conversely, this Note offers a novel perspective and solution, benefitting from the insight of how two circuit courts grappled with the issue. The solution this Note provides is thus both informed by and responsive to the reasoning of the Fifth and Fourth Circuits. As a result, the Purpose-

43. Karen Gullo, *Location Data Tracks Abortion Clinic Visits. Here's What to Know*, ELEC. FRONTIER FOUND. (Mar. 15, 2024), https://www.eff.org/deeplinks/2024/03/location-data-tracks-abortion-clinic-visits-heres-what-know [https://perma.cc/3NUN-JDQ9].

44. *See generally* Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SEC. & POL'Y 247 (2016); Charlie Brownstein, *Confronting* Carpenter*: Rethinking the Third-Party Doctrine and Location Information*, 92 FORDHAM L. REV. 183 (2023); Tonja Jacobi & Dustin Stonecipher, *A Solution for Third-Party Doctrine in a Time of Data Sharing, Contact Tracing, and Mass Surveillance*, 97 NOTRE DAME L. REV. 823 (2022); Margaret E. Twomey, *Voluntary Disclosure of Information as a Proposed Standard for the Fourth Amendment's Third-Party Doctrine*, 21 MICH. TELECOMM. & TECH. L. REV. 401 (2015).

Sensitivity approach is more workable and more likely to be adopted than other proposals.[45]

This Note proceeds in four parts. Part I introduces and explains third-party doctrine, with a focus on its critiques and an explanation of how it led to *Carpenter*. Part II then details the Court's decision in *Carpenter* and explains the circuit split by analyzing each lower court's decision and the Fourth Circuit's en banc decision. Through this analysis, this Part shows how lower courts have struggled to apply *Carpenter* and third-party doctrine. It then ends with a discussion of the scholarly responses to *Carpenter*, explaining how they fall short in light of the circuit split and how this Note responds to the scholarly shortcomings. Part III then details this Note's Purpose-Sensitivity approach and applies it, with a focus on how it responds to the circuit court decisions. Part IV of the Note defends the practicality of the Purpose-Sensitivity approach by highlighting how it flows from the Court's Fourth Amendment and third-party jurisprudence, is in line with the text of the Fourth Amendment, and is responsive to concerns with third-party doctrine. The Note concludes by discussing the timeliness and necessity of the Purpose-Sensitivity approach.

I. THIRD-PARTY DOCTRINE IS UNWORKABLE FOR LOCATION DATA

A. History of Third-Party Doctrine

Third-party doctrine arose out of two cases, the first being *United States v. Miller*.[46] *Miller* concerned a government investigation of Mitch Miller for tax evasion, which resulted in a subpoena of his banks for multiple months of canceled checks, deposit slips, and monthly statements.[47] The Court determined that these actions did not constitute a Fourth Amendment violation for two reasons. First, Miller could "assert neither ownership nor possession" of the documents requested because he did not own them, as they were "business records of the banks."[48] Second, the nature of the documents sought implicated very limited privacy concerns because they

45. At the time of this writing, the Court has granted certiorari in *Chatrie*. Argument has been scheduled for April 27, 2026. United States v. Chatrie, 136 F.4th 100 (4th Cir. 2025) (en banc) (per curiam), *cert. granted*, No. 25-112, 2026 U.S. LEXIS 705 (U.S. Jan. 16, 2026).

46. 425 U.S. 435 (1976).

47. *Id*. at 435.

48. *Id*. at 440.

were "not confidential communications but negotiable instruments to be used in commercial transactions" and "exposed to [bank] employees in the ordinary course of business."[49] The Court therefore concluded that Miller had "take[n] the risk, in revealing his affairs to another, that the information [would] be conveyed by that person to the Government."[50] And so, third-party doctrine was born.

The Court further expanded upon third-party doctrine in *Smith v. Maryland*. In *Smith*, the police requested that a telephone company install a pen register to record numbers called from Michael Lee Smith's phone. The Court held that this did not constitute a search protected by the Fourth Amendment. The Court focused this inquiry on whether Smith could claim a reasonable expectation of privacy. It determined that he had no expectation of privacy and that even if he did, it was not reasonable. First, the Court decided that because of the pen register's "limited capabilities," there was "doubt that people in general entertain any actual expectation of privacy in the numbers they dial."[51] This is because users know that the numbers are used "for a variety of legitimate business purposes" such as determining if the phone is being used for business or personal reasons.[52] The Court then turned to third-party doctrine and said that even if Smith had a subjective expectation of privacy, it is not recognized as reasonable because he conveyed the information to a third party.[53] It reasoned that Smith "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business," and in the process he "assumed the risk that the company would reveal to police the numbers he dialed."[54] As such, the Court held that Smith did not have a Fourth Amendment–protected privacy right in the telephone numbers he dialed.[55]

The important impact of these two cases is the test they created. As applied by the Court, third-party doctrine states that there is no reasonable expectation of privacy in information one "knowingly and voluntarily" exposes to third parties. Today, when lower courts are faced with a Fourth Amendment challenge, they start by determining if the information was

49. *Id*. at 442.

50. *Id*. at 443.

51. Smith v. Maryland, 442 U.S. 735, 742 (1979).

52. *Id*. at 743.

53. *Id*. at 744.

54. *Id*.

55. *Id*. at 745.

knowingly and voluntarily shared with a third party. If it was, then third-party doctrine applies; there is no reasonable expectation of privacy and therefore no Fourth Amendment protection. The next Section explains the scholarly critiques of third-party doctrine, setting the stage for how *Carpenter* failed to address them and showing that a new intervention is needed.

B. Critiques of Third-Party Doctrine

Third-party doctrine was criticized when it was first developed, but in the digital age its critiques increased.[56] Prior to *Carpenter*, scholars and judges alike argued that third-party doctrine was unworkable in the digital age. Scholars have two primary critiques. The first is that with modern technology, so much of our traditionally private data is shared with third parties, so third-party doctrine will lead to the erosion of the Fourth Amendment. The second is that in the digital age people have little choice but to share their private information with third parties, because sharing is required to participate in modern life.

Even in the early 2000s, many scholars argued that with third-party doctrine, Fourth Amendment protections would soon have no effect because so much of our private information is in the hands of third parties. For example, in 2005, Daniel J. Solove spoke of Internet service providers and the bookstore "Amazon.com," writing that "third party doctrine presents one of the most serious threats to privacy in the digital age."[57] Little did Solove know that just 20 years later, technology would balloon and Amazon would have access to even more of our data, far beyond our book preferences. As Matthew Tokson wrote, "[T]he Internet has begun to reshape . . . practically every aspect of modern life, [and] we appear to be racing towards another enormous gap in legal protection for private communications."[58] Other scholars echoed this concern and commented that because of "rapid advances in information technology and a

56. Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 585 (2011) (explaining that "[w]hile Smith and the Third Party Doctrine were heavily criticized even before the Internet age, the drumbeat of criticism has intensified").

57. Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 753 (2005).

58. *See* Tokson, *supra* note 56, at 584.

proliferation of third-party records," the Fourth Amendment's privacy protections were being winnowed away.[59]

Another common concern is that in the modern technological age, "people have no choice but to share records and data with third parties."[60] Scholars recognize that "our lives are lived with the assistance and mediation of digital platforms" and that the use of these digital platforms is required to participate in society.[61] This is concerning because under third-party doctrine, a "[c]onsumer actually has no choice but to forego privacy expectations unless he is willing to forego a material, if not practically essential, service."[62] Even Justice Sotomayor, prior to *Carpenter*, said third-party doctrine "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[63]

The ambiguity and nonadministrability of third-party doctrine played out over time, leading many scholars and practitioners to call for the Court to weigh in. These scholars wanted the Court to address how to apply third-party doctrine in the digital age. Many specifically advocated for the Court to either overturn third-party doctrine or make it clearer.[64] It was against this backdrop that the Court heard *Carpenter v. United States*. But as the next

59. Price, *supra* note 44, at 247.

60. Daniel Solove, *10 Reasons Why the Third Party Doctrine Should Be Overruled in* Carpenter v. US, TEACHPRIVACY (Nov. 28, 2017), https://teachprivacy.com/carpenter-v-us-10-reasons-fourth-amendment-third-party-doctrine-overruled/ [https://perma.cc/B32P-XAX2]. Other courts before *Carpenter* had decided that digital data was distinguishable from *Smith* and *Miller* and thus third-party doctrine did not apply. *See, e.g.*, United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) (explaining that emails stored on an Internet service provider are not subject to third-party doctrine).

61. Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139, 144-45 (2016).

62. Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J. L. & POL'Y 211, 244 (2006). As discussed in Section III.C, the Purpose-Sensitivity test eliminates the need for analyzing the necessity of sharing for daily life. This test re-anchors third-party doctrine in its original purpose and in the intent of the Fourth Amendment. *See also infra* note 184.

63. United States v. Jones, 565 U.S. 400, 414 (2012) (Sotomayor, J., concurring).

64. *See, e.g.*, Tokson, *supra* note 56, at 584-85, 634-35; Price, *supra* note 44, at 268-69; Lucas Issacharoff & Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 987, 994-98 (2016).

Part shows, *Carpenter* did not provide the much-needed clarity, and in its wake courts have been unsure of how to apply third-party doctrine, as evidenced by the circuit split.

II. THE CURRENT PROBLEM: *CARPENTER* AND ITS CHAOS

In the modern era, the Court has only examined third-party doctrine as it relates to location data once—in *Carpenter*.[65] Through this case, the Court addressed whether third-party doctrine extended to cell site location information,[66] determining it does not. This Part details the Court's reasoning and rationale for not extending third-party doctrine to CSLI. It then explains how the Court's concerns with CSLI apply to location data broadly. While *Carpenter* provided useful dicta and analysis, this Part highlights the confusion it created over whether and how third-party doctrine should extend to location data. Accordingly, this Note argues that third-party doctrine is currently unworkable for location data and that a new test is needed, which is further highlighted by the circuit split and the granted cert petition in *Chatrie*.

A. The *Carpenter* Exception

Carpenter arose out of a series of robberies in which the police suspected Timothy Carpenter. The prosecutors in the case applied for Carpenter's cell site records under the Stored Communications Act, which permits "the Government to compel the disclosure of certain telecommunications records when it 'offers specific and articulable facts showing that there are reasonable grounds to believe' that the records sought 'are relevant and material to an ongoing criminal investigation.'"[67] A judge issued the two orders and Carpenter's wireless carriers disclosed his cell site location information for incoming and outgoing calls during the four-month time period when the robberies occurred. The government received "12,898 location points cataloging Carpenter's movements—an average of 101 data points per day."[68] Using this information the

65. However, the Court has recently agreed to hear *Chatrie*. *See supra* note 45.

66. For a definition of cell site location information, *see supra* note 15 and accompanying text.

67. Carpenter v. United States, 585 U.S. 296, 302 (2018) (quoting 18 U.S.C. § 2703(d)).

68. *Id.*

government charged Carpenter with six counts of robbery and six acts of carrying a firearm during a federal crime of violence.[69] Carpenter appealed to suppress the cell site location information, arguing that the search violated his Fourth Amendment rights. The Sixth Circuit rejected his argument and affirmed the lower court, determining that Carpenter "lacked a reasonable expectation of privacy in the location information collected by the FBI because he had shared that information with his wireless carriers."[70] The Sixth Circuit reasoned that Carpenter had voluntarily given his cell site location information to his carriers and thus was not entitled to Fourth Amendment protection under the third-party doctrine.[71] The Supreme Court granted cert.

After a discussion of the history and intent of the Fourth Amendment, the Court turned to the heart of the case: third-party doctrine. When deciding whether Fourth Amendment protections are waived through third-party doctrine, the Court looks at whether a person "knowingly and voluntarily" gave their information to a third party. Here, the majority admitted that this case does not neatly fit into the precedent that informs third-party doctrine. The Court had two main concerns: first, how much information can be conveyed by CSLI, and second, whether "voluntarily" and "knowingly" can be applied to CSLI. The Justices explained that when the Court created third-party doctrine, it applied the doctrine to telephone numbers and bank records, which reveal "little in the way of 'identifying information.'"[72] The Court conceded that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[73] That remains true "even if the information is revealed on the assumption that it will be used only for a limited purpose."[74] "As a result, the Government is typically free to obtain such information from the recipient without triggering Fourth Amendment protections."[75] However, CSLI does not conform to this paradigm because it is a "qualitatively

69. *Id.*

70. *Id.* at 303.

71. *Id*.

72. *Id*. at 314 (first citing Smith v. Maryland, 442 U.S. 735, 742 (1979); then citing and quoting Riley v. California, 573 U.S. 373, 400 (2014)).

73. *Smith*, 442 U.S. at 743-44.

74. United States v. Miller, 425 U.S. 435, 443 (1976).

75. *Carpenter*, 585 U.S. at 303.

different category."[76] As such, the Court declined to extend third-party doctrine to CSLI, thereby creating a narrow exception wherein CSLI—but only CSLI—is no longer subject to third-party doctrine.

Due to the difficulty in applying third-party doctrine and its reluctance to rely on it,[77] the Court instead leaned largely on other Fourth Amendment jurisprudence. First, the Court explained *United States v. Knotts*,[78] where a beeper was attached to track a vehicle through traffic. There the Court determined that the beeper was rudimentary technology with limited uses, so it was not a Fourth Amendment–protected search. Next, the Court discussed *United States v. Jones*,[79] where the Court determined that the FBI violated the Fourth Amendment when agents used a GPS tracking device on a car to monitor a vehicle's movements for twenty-eight days. Importantly, the Court in *Carpenter* distinguished its holding from the decision in *Knotts*. The Court used *Jones* to explain that its precedent made clear that location tracking infringes on an expectation of privacy when it is more sophisticated.[80] Thus in *Carpenter*, the Court determined that "[m]uch like GPS tracking of a vehicle, cell site location information is detailed, encyclopedic, and effortlessly compiled."[81]

Based on precedent, the Court declined to extend third-party doctrine to CSLI. The Court reasoned that while "the fact that the individual continuously reveals his location to his wireless carrier implicates the third-party principle of *Smith* and *Miller*," it is not clear that third-party doctrine applies to cell site records.[82] This is because when *Smith* and *Miller* were decided "few could have imagined a society in which a phone goes" everywhere and creates a detailed record of a user's life.[83] So in the end, the Court created an exception to third-party doctrine, deciding not to extend it to CSLI because it was not clear whether the information was "knowingly and voluntarily" shared, and because CSLI concerned more sensitive and private information than *Smith* and *Miller*.

---

76. *Id*.

77. The Justices identified that third-party doctrine was difficult to apply to location data because determining whether something is "knowingly and voluntarily exposed" is complicated. *See id.*

78. 460 U.S. 276 (1983).

79. 565 U.S. 400 (2012).

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

81. *Id*. at 309.

82. *Id.* at 297.

83. *Id.* at 309.

1. Similarities between CSLI and Location Data

Carpenter explains why third-party doctrine is ill-suited for the technological age and for CSLI in particular. *Carpenter*'s analysis also proves that the doctrine is unworkable for location data, which is why this Note proposes the Purpose-Sensitivity approach for all location data shared with a third party. *Carpenter*'s holding applies narrowly to CSLI collected by the government from cell phone companies. Location data, the focus of this Note, refers to all kinds of location information the government might collect and search from a wide-ranging number of companies who track their customers. This Section argues that the concerns about CSLI are the same, stronger even, for location data. The difference between CSLI and location data is that the former only collects location information when a cell phone connects to a tower or network, whereas the latter collects it continuously.[84] Location data creates an even more detailed and precise chronicle of a person's location than the Court was concerned about in *Carpenter*. Additionally, location data raises the same concerns as CSLI over whether a user "knowingly and voluntarily" shared their information with a third party. Much like CSLI, the opt-in process is often confusing and ill-informed.[85] While there may be concerns with third-party doctrine and data generally, this Note focuses on location data because the concerns that the Court had about CSLI apply to location data, and because third-party doctrine has proven unworkable for location data specifically.

In terms of privacy, both CSLI and location data have similar concerns that make them a poor fit for third-party doctrine. In *Carpenter*, the Justices highlighted that the information sought in *Smith* and *Miller* was "limited types of personal information."[86] Conversely, CSLI "is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years. Such a chronicle implicates privacy concerns

84. *See supra* notes 15 and 23 and accompanying text.

85. *See* Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1884-88 (2013) (explaining the many barriers to consent including misunderstanding and misinformation); Hannah J. Hutton & David A. Ellis, *Exploring User Motivations Behind iOS App Tracking Transparency Decisions*, PROCS. OF THE 2023 CHI CONF. ON HUM. FACTORS IN COMPUTING SYS. 1, 7-8 (Apr. 2023), https://dl.acm.org/doi/pdf/10.1145/3544548.3580654 [https://perma.cc/5SE8-AMBT] (explaining that users have misconceptions about tracking and think that tracking will benefit them, but do not understand the risks associated with tracking).

86. *Carpenter*, 585 U.S. at 297.

far beyond those considered in *Smith* and *Miller*."[87] Similarly, the location data shared with third parties today is in no way limited, as cell phones track our every move. As the Fifth Circuit explained, this location data "exemplif[ies] the Court's concern with pinpoint location data—this technology provides more precise location data than either CSLI or GPS."[88] As such, the Court's privacy concerns with CSLI map onto location data broadly.

Another aspect of privacy within third-party doctrine is whether the information is "knowingly and voluntarily" shared. The Court was clear in *Carpenter* that "[t]he third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another."[89] The Court based this reasoning on earlier precedent that highlighted the balance struck between knowingly sharing information and maintaining privacy.[90] Third-party doctrine was focused on information that was shared with little privacy concerns. Location data is entirely different, because it has greater privacy implications and is not "knowingly" shared in the same way.[91] Therefore, the Court's concerns that

87. *Id*. at 315.

88. United States v. Smith, 110 F.4th 817, 833 (5th Cir. 2024), *cert. denied*, No. 24-7237, 2025 U.S. LEXIS 4192 (U.S. Nov. 10, 2025).

89. *Carpenter*, 585 U.S. at 298.

90. For example, the Court explained that "*Smith* pointed out the limited capabilities of a pen register; as explained in *Riley*, telephone call logs reveal little in the way of 'identifying information.' *Miller* likewise noted that checks were 'not confidential communications but negotiable instruments to be used in commercial transactions.'" *Id.* at 314 (citations omitted) (first citing Smith v. Maryland, 442 U.S. 735, 742 (1979); then citing and quoting Riley v. California, 573 U.S. 373, 400 (2014); and then citing and quoting United States v. Miller, 425 U.S. 435, 442 (1976)).

91. Justice Alito has recognized the greater privacy implications of location data:

> In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention. GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. *See, e.g.*, *People v. Weaver*, 12 N.Y. 3d 433, 441–442 (2009) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense

CSLI may not be "knowingly and voluntarily" shared follow for location data generally.

As the Court explained in *Carpenter*, the nature of sharing location data is different from sharing as third-party doctrine initially conceived it. The majority wrote that "[c]ell phone location information is not truly 'shared' as one normally understands the term."[92] This concern with CSLI again clearly tracks onto location data broadly. The Court did note that there was no affirmative act on the part of the user in *Carpenter*, whereas with location data this is less clear, as seen from the circuit courts. However, as the majority in *Carpenter* points out, the voluntariness of sharing is questionable when cell phones and the services they provide are "'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[93] This rings even truer today when cell phones are completely embedded in daily life, as is using the applications on them that require you to give your location information to third parties.

2. Lessons from *Carpenter*

The Court's decision not to extend third-party doctrine in *Carpenter* exemplifies why third-party doctrine is unworkable for location data. Location data, like cell site location information, concerns privacy interests, is comprehensive, and is not given knowingly and voluntarily. The circuit split between the Fourth and Fifth Circuits further elucidates the comparisons between CSLI and location data, exemplifying why third-party doctrine as it stands should not apply to the latter. As the split also shows, *Carpente*r created a narrow carve out to third-party doctrine that failed to provide lower courts with clear guidance on how to use the doctrine in the technological era. Instead, *Carpenter* left lower courts more confused over how, if at all, to apply third-party doctrine.

B. In the Cracks Left by *Carpenter*, a Split Emerges

Both the Fourth and Fifth Circuits were faced with the question of whether the Fourth Amendment protects location data shared with a third

attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on").

United States v. Jones, 565 U.S. 400, 415 (2012) (Alito, J., concurring) (citation modified).

92. *Carpenter*, 585 U.S. at 315.

93. *Id.* at 298 (quoting *Riley*, 573 U.S. at 385).

party, specifically location data collected by a "geofence warrant," which is not a typical warrant, but a request to companies from law enforcement for location data.[94] Both courts relied on *Carpenter* and third-party doctrine but reached different conclusions about whether the doctrine applied and whether a Fourth Amendment–protected search had occurred. This Note argues that this discrepancy highlights how third-party doctrine is unworkable for location data. Further, this Note argues that the Fifth Circuit majority and the original Fourth Circuit dissent explain why the reasoning in *Carpenter* and discussion of CSLI is analogous to location data.[95] However, unlike the Fifth Circuit, this Note does not rely on a *Carpenter*-like analysis to determine whether third-party doctrine applies to each individual location data case. Instead, in Part III, this Note presents a new test for location data that is shared with third parties. This new test is informed by and responsive to the Fourth and Fifth Circuit decisions—addressing the concerns put forth by the judges and relying on their explanations and reasoning.[96]

1. Fourth Circuit: *Chatrie*

On July 9, 2024, the Fourth Circuit, in a split decision, ruled that the government's use of a geofence warrant did not constitute a Fourth Amendment–protected search in *United States v. Chatrie*.[97] The case stemmed from a bank robbery in 2019.[98] In this case, the government obtained a geofence warrant to acquire Google's Location History data, a

94. *See supra* note 8. The difference between a normal search warrant and a geofence warrant is that for a search warrant police need probable cause related to a suspect, and with a geofence warrant they just need probable cause related to an area; this is why many have argued that geofence warrants are unconstitutional general warrants. Navdeep Kaur Bal, *The Constitutionality of Geofence Warrants*, BERKELEY J. CRIM. L.: BLOG (Jan. 18, 2024), https://www.bjcl.org/blog/the-constitutionality-of-geofence-warrants/ [https://perma.cc/PV4V-276H].

95. *See supra* note 23 for a definition of CSLI and discussion of the difference between CSLI and location data.

96. *See infra* Section III.C.

97. 107 F.4th 319, 332 (4th Cir. 2024), *aff'd on reh'g en banc*, 136 F.4th 100 (4th Cir. 2025) (per curiam), *cert. granted*, No. 25-112, 2026 U.S. LEXIS 705 (U.S. Jan. 16, 2026).

98. *Id.* at 324.

digital log of users' movements,[99] for devices in a 150-meter radius of the bank robbery beginning 30 minutes before the robbery and ending 30 minutes after the robbery.[100] From this information, the government narrowed the list of suspects and then requested a smaller number of devices' Location History from one hour before to one hour after the robbery.[101] After law enforcement narrowed the list further, Google provided the identity information associated with each of the devices.[102] This led the government to Okello Chatrie, the appellant in this case.[103] Chatrie pleaded not guilty, and subsequently moved to suppress the evidence obtained via the geofence warrant for violating his Fourth Amendment rights.[104] The district court denied Chatrie's motion to suppress in 2022.[105] After conditionally pleading guilty and being sentenced, Chatrie appealed to the Fourth Circuit.[106]

On appeal, Chatrie argued that the geofence warrant violated his Fourth Amendment rights and therefore the evidence should be suppressed.[107] Chatrie based his claims on a reasonable expectation of privacy in his location data.[108] The Fourth Circuit, initially, found this argument unconvincing and asserted that Chatrie did not have a reasonable expectation of privacy in his data.[109]

The Fourth Circuit, originally, largely relied on the third-party doctrine in concluding that the government did not engage in a Fourth Amendment–

99. *Id.* at 322 (explaining that "Location History is an optional account setting that allows Google to track a user's location while he carries his mobile devices. If a user opts in, Google keeps a digital log of his movements and stores this data on its servers, and that a user can opt in "either through an internet browser, a Google application (such as Google Maps), or his device settings (for Android devices).").

100. *Id.* at 324.

101. *Id.* at 325.

102. *Id.*

103. *Id.*

104. *Id.* at 321-22.

105. *Id.* at 325.

106. *Id.*

107. *Id.*

108. *Id.* at 325.

109. *Id*. at 332.

protected search.[110] Relying on *Carpenter*, the judges identified two rationales for extending third-party doctrine to location data collected by a geofence warrant.[111] First, they decided the information sought did not implicate privacy concerns, and second, that Chatrie voluntarily exposed the information to a third party.[112] They focused on the fact that the Location History covered a short time and therefore did not provide insight into private details of Chatrie's life.[113] They also focused on Chatrie's consent to using Google Location History.[114] Conversely to the Fifth Circuit, the Fourth Circuit decided it was clear that Chatrie had knowingly and voluntarily exposed his location information.[115]

The original dissent in the Fourth Circuit disagreed with the two rationales the majority pulled from *Carpenter*. Instead, the dissent asserted that there are five *Carpenter* factors that the majority should have

110. *Id.*

111. *Id*. at 326.

112. *Id*. at 330-31.

113. *Id.* at 330.

114. *Id*. at 331.

115. *Id.* The Fifth Circuit and scholars have expressed concern with the reasoning the Fourth Circuit used to decide that Chatrie "knowingly and voluntarily exposed" his location information. *See* United States v. Smith, 110 F.4th 817, 835-36 (5th Cir. 2024), *cert. denied*, No. 24-7237, 2025 U.S. LEXIS 4192 (U.S. Nov. 10, 2025); Carpenter v. United States, 585 U.S. 296, 298 (2018) ("Cell phone location information is not truly 'shared' as the term is normally understood. First, cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society. Second, a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the user's part beyond powering up." (citation omitted) (citing Riley v. California, 573 U.S. 373, 385 (2014)); *In re* Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 737 (N.D. Ill. 2020) ("The Court finds it difficult to imagine that users of electronic devices would affirmatively realize, at the time they begin using the device, that they are providing their location information to Google in a way that will result in the government's ability to obtain – easily, quickly and cheaply – their precise geographical location at virtually any point in the history of their use of the device."); Solove, *supra* note 85, at 1884-88 (explaining the many barriers to consent, including misunderstanding and misinformation); Hutton & Ellis, *supra* note 85, at 7-8 (explaining that users have misconceptions about tracking and think that tracking will benefit them, but do not understand the risks associated with tracking).

applied.[116] The first is the comprehensiveness of the intrusion, which involves looking at both the depth and breadth of the search.[117] The second factor is the retrospective capabilities of the intrusion.[118] The third factor is intimacy, the fourth is ease of access, and the fifth is voluntariness.[119] Addressing each factor in turn, the dissent determined that each supports the conclusion that third-party doctrine does not cover geofence location data and that the search violated the Fourth Amendment.[120] In many ways, the dissent's reasoning mirrors *Carpente*r, highlighting how CSLI and geofence location data are analogous in ways that make it clear the third-party doctrine should not extend to location data.[121]

Importantly in the Fourth Circuit opinion, the tension between the majority and dissent stems from disagreements over the reasoning and application of *Carpenter*. While the majority found that *Carpenter* set out a two-prong rationale, the dissent found that it gave a five-factor test. The majority ruled that the location data did not implicate privacy concerns because it was not comprehensive or intimate. Conversely, the dissent found that location data provided the government with a detailed and intimate look into Chatrie's private information. The majority also concluded that Chatrie shared the information voluntarily, while the dissent argued that even if Chatrie did consent, the information was not truly shared voluntarily.

Following this decision, the Fourth Circuit reheard *Chatrie* en banc, and the result made it even more evident that *Carpenter* left lower courts with an unworkable third-party doctrine. The per curiam decision is only a few words in length, saying, "PER CURIAM: The judgment of the district court is AFFIRMED."[122] The affirmed lower-court decision also could not decide whether third-party doctrine applied, and instead found that the good faith exception applied.[123] What follows is 124 pages of separate opinions that

116. *Chatrie*, 107 F.4th at 346 (Wynn, J., dissenting).

117. *Id*. at 346-47 (Wynn, J., dissenting).

118. *Id*.

119. *Id.*

120. *Id*. at 348-61 (Wynn, J., dissenting).

121. *Id*.

122. United States v. Chatrie, 136 F.4th 100, 101 (4th Cir. 2025) (en banc) (per curiam), *cert. granted*, No. 25-112, 2026 U.S. LEXIS 705 (U.S. Jan. 16, 2026).

123. United States v. Chatrie, 590 F. Supp. 3d 901, 935 (E.D. Va. 2022) ("At base, [applying third-party doctrine] is complex. And considering the messiness of the current record as to how and when Chatrie 'gave consent,' the Court

show just how unclear *Carpenter* is and how third-party doctrine is unworkable for location data.

Specifically, the decision was accompanied by seven concurrences and one dissent. The concurrences range in opinion from the good faith exception applies, so none of the reasoning matters,[124] to third-party doctrine applies and geofencing is not a search,[125] to third-party doctrine does not apply and geofencing is a search.[126] The judges specifically struggled to apply *Carpenter*. One group of judges found that *Carpenter* replaced third-party doctrine and created a new multifactor test.[127] A different group found that *Carpenter* created a two-factor test.[128] Another group found that *Carpenter* left third-party doctrine intact and it is still good law.[129] And yet another group of judges found that *Carpenter* limited third-party doctrine, but under *Carpenter* third-party doctrine still applies here.[130]

The divergence in understanding and application of *Carpenter* in the first Fourth Circuit opinion and in the concurrences on rehearing highlights the difficulty in applying precedent related to third-party doctrine to location data, and demonstrates how the doctrine is unworkable for location data. Further, the dissent in the original case shows how CSLI is

---

cannot—and need not—reach a firm decision on the issue. But the Court remains unconvinced that the third-party doctrine would render hollow Chatrie's expectation of privacy in his data, even for 'just' two hours."), *aff'd*, 107 F.4th 319 (4th Cir. 2024), *and aff'd on reh'g en banc*, 136 F.4th 100 (4th Cir. 2025) (per curiam), *cert. granted*, No. 25-112, 2026 U.S. LEXIS 705 (U.S. Jan. 16, 2026). The good faith exception allows "courts to admit unlawfully collected evidence if the police can show they relied in good faith on existing authority." Matthew Tokson & Michael Gentithes, *The Reality of the Good Faith Exception*, 113 GEO. L. J. 551, 551 (2025).

124. *Chatrie*, 136 F.4th at 101 (Diaz, J., concurring).

125. *Id.* at 109 (Wilkinson, Niemeyer, King, Agee & Richardson, JJ., concurring).

126. *Id.* at 115 (Wynn, Thacker, Harris, Benjamin & Berner, JJ., concurring) (Gregory, J., concurring in part).

127. *Id*. at 120-21.

128. *Id.* at 143 (Berner, Gregory, Wynn, Thacker & Benjamin, JJ., concurring) (Heytens, J., concurring in part).

129. *Id.* at 110 (Wilkinson, Niemeyer, King, Agee & Richardson, JJ., concurring).

130. *Id.* at 138-39 (Richardson, Wilkinson, Niemeyer, King, Agee, Quattlebaum & Rushing, JJ., concurring).

analogous to location data. The Fifth Circuit fared no better, similarly struggling to make sense of *Carpenter* and third-party doctrine.

2. Fifth Circuit: *Smith*

A month after the Fourth Circuit originally found that third-party doctrine applied to a geofence warrant, the Fifth Circuit held the opposite in *United States v. Smith*.[131] The case arose from the robbery of a United States Postal Service driver in 2018.[132] Nine months after the robbery, the police did not have any suspects, so they requested a geofence warrant to help them identify possible suspects.[133] On the first step, the warrant produced an hour's worth of data from Google covering 378,278 square meters around the post office.[134] The police then requested location information for a longer period of time for three devices and the identifying information for those three devices.[135] The three defendants were then arrested and charged.[136] At the district court level, they filed a motion to suppress the geofence data, which the court denied.[137] The court found the defendants guilty and sentenced them to prison.[138] The defendants subsequently appealed to the Fifth Circuit.[139]

At the Fifth Circuit, the three appellees argued they had a reasonable expectation of privacy in their location data and therefore the data was protected by the Fourth Amendment.[140] The Fifth Circuit found this argument convincing and based its reasoning largely on *Carpenter*.[141] The court compared the appellees' location data to the data collected in

131. 110 F.4th 817 (5th Cir. 2024), *cert. denied*, No. 24-7237, 2025 U.S. LEXIS 4192 (U.S. Nov. 10, 2025).

132. *Id*. at 820.

133. *Id*. at 821.

134. *Id*. at 827-28.

135. *Id*. at 828.

136. *Id.* at 829.

137. *Id*.

138. *Id*. at 830.

139. *Id*.

140. *Id*. at 831.

141. *Id*. at 831-35.

Carpenter and found that it was very similar and thus was protected by a reasonable expectation of privacy.[142]

Unlike the Fourth Circuit in its original decision, the Fifth Circuit found that third-party doctrine did not extend to geofence location data. Again, the Fifth Circuit based its reasoning on *Carpenter*, where the Court similarly declined to extend third-party doctrine. The judges found that CSLI and geofence location data were analogous for the purposes of third-party doctrine.[143] The Fifth Circuit identified specific concerns with third-party doctrine that the Justices pointed to in *Carpenter*, such as the comprehensive nature of the data and the permeating police surveillance that access to location data could create.[144] Accordingly, the Fifth Circuit parted ways with the Fourth Circuit's original decision, holding that third-party doctrine did not extend to location data because the intrusiveness of even a limited amount of location data was too great.[145]

Further, the Fifth Circuit split from the Fourth Circuit's original decision by denying that Smith had "knowingly and voluntarily" shared his data with a third party.[146] The court reasoned that the "opt-in" process with location data is "hardly informed, and in many instances, may not even be voluntary" and that there is "ubiquity—and necessity—in the digital age of entrusting corporations like Google, Microsoft, and Apple with highly sensitive information."[147] Assuming that users voluntarily give their information "is dubious."[148]

As such, the Fifth Circuit found that Smith did have a reasonable expectation of privacy in his location data because it was intrusive and ubiquitous. Beyond that though, the court found that *Carpenter* instructed it not to extend third-party doctrine to the location data gathered by a geofence warrant.[149] This is particularly interesting because the Fourth Circuit, in its first decision, also relied on *Carpenter* to examine geofence warrants and found that they were covered by third-party doctrine and that a Fourth Amendment–protected search had not occurred. Though the two

142. *Id.* at 834-36.

143. *Id*.

144. *Id*. at 833.

145. *Id*.

146. *Id*. at 835-36.

147. *Id*. at 835.

148. *Id*.

149. *Id*. at 836.

courts disagreed on most aspects of the analysis, a key takeaway from the two original decisions is that relying on *Carpenter* led the courts to two different outcomes. *Carpenter* created a narrow exception to third-party doctrine for CSLI, but left the doctrine intact without explaining how, if at all, to extend it to location data generally. It is this issue that this Note addresses with its novel approach to third-party doctrine.

3. Lessons from the Circuit Courts

The original split between the Fifth and Fourth Circuits and the indecision of the Fourth Circuit on rehearing shows that third-party doctrine does not easily extend to location data. This Note agrees with the Fifth Circuit's conclusion. However, this Note argues that the lack of clarity on how to apply third-party doctrine post-*Carpenter* meant that the doctrine as it currently exists was unhelpful to the Fifth Circuit in reaching its decision. The difference between the Fifth and original Fourth Circuit holdings regarding whether the information was "knowingly and voluntarily" exposed demonstrates that third-party doctrine is unworkable for location data. Additionally, the difference in determinations on reasonable expectation of privacy also shows that third-party doctrine is not feasible in the location-data context. The new Fourth Circuit decision, or lack thereof, and the inability of the court to reach a consensus highlights the difficulty in interpreting *Carpenter* and applying third-party doctrine to location data.

C. Scholarly Responses and the Problem with "Knowingly and Voluntarily Exposed"

As the circuit split shows, *Carpenter* had many shortcomings. One of the biggest challenges for the circuit courts was applying the "knowingly and voluntarily exposed" test. Scholarly responses to *Carpenter* fall short because they do not address this particular issue, and their proposals utilize the "knowingly and voluntarily exposed" test. Because the primary scholarly responses came before *Chatrie* and *Smith*, they did not understand the challenge lower courts face in applying "knowingly and voluntarily exposed" in the digital age. Conversely, this Note proposes a new test that does not rely on "knowingly and voluntarily exposed" and is instead rooted in both the circuit court decisions and *Carpenter*. As such, this Note's approach is workable for lower courts. To explain the shortcomings of the scholarly responses, this Section begins by showing how "knowingly and voluntarily exposed" is unworkable in the digital age. It then discusses three

of the main scholarly responses to *Carpenter*, showing how they are not practicable. It concludes by explaining how the proposed test does not rely on "knowingly and voluntarily exposed" and is feasible.

The primary inquiry of third-party doctrine is to determine if the information collected and searched by the government was "knowingly and voluntarily exposed." Today, neither factor operates as intended for location data. First, many would contend that the notion that information is voluntarily shared is an illogical proposition when sharing is required by society to participate in daily life. Second, because opt-in and consent procedures are unclear and confusing, many scholars and practitioners argue that users do not knowingly and voluntarily consent to sharing their location data.[150]

It is axiomatic that sharing data with third parties is a required part of daily life. Many Justices have expressed this very fact. Justice Sotomayor warned that the Court may need "to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[151] She reasoned that "[t]his approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[152] This rationale is part of the reason the Fifth Circuit, in *Smith*, did not apply third-party doctrine. Instead the Fifth Circuit determined that "[g]iven the ubiquity—and necessity—in the digital age of entrusting corporations like Google, Microsoft, and Apple with highly sensitive information, the notion that users voluntarily relinquish their right to privacy and 'assume[] the risk' of this information being divulged to law enforcement is dubious."[153] Justice Gorsuch similarly explained in his *Carpenter* dissent, "Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers. *Smith* and *Miller* say that the police can review

150. *See supra* note 85; *see also Smith*, 110 F.4th at 835 ("These requests typically innocuously promise app optimization, rather than reveal the fact that users' locations will be comprehensively stored in a 'Sensorvault,' providing Google the means to access this data and share it with the government. . . . Even Google's own employees have indicated that deactivating Location History data based on Google's 'limited and partially hidden' warnings is 'difficult enough that people won't figure it out.'").

151. United States v. Jones, 565 U.S. 400, 417 (2012).

152. *Id.*

153. *Smith*, 110 F.4th at 835 (citing Smith v. Maryland, 442 U.S. 735, 745 (1979)).

all of that data on the theory that no one reasonably expects any of it will be kept private."[154]

In *Smith* and *Miller*, the Court reasoned that the petitioners knew their respective information would be shared with third parties. Smith was aware that banks share documents in the course of business and Miller knew that telephone companies also shared numbers dialed to conduct business. This is not analogous to location data or to the technological age we live in today. When people use Google Maps or enable location services on other apps, it is likely they are unaware that they are consenting to the collection and storage of their location data. Are you aware of all the apps that are tracking you?

Despite this, Orin S. Kerr, one of the main defenders of third-party doctrine, relies heavily on the validity of the "knowingly and voluntarily exposed" test. In particular, he argues that third-party doctrine should be understood as a consent doctrine and that "[t]hird-party disclosure eliminates privacy because the target voluntarily consents to the disclosure."[155] With this understanding, he says it is clear that third-party doctrine is workable and does not give the government too much power beyond that consented to by the user.[156] A similar but broader proposal is put forth by Matthew J. Tokson. He argues that *Carpenter* should be the guiding Fourth Amendment test for searches.[157] Specifically, he asserts that the *Carpenter* factors, including voluntariness, "appear to be workable for judges."[158] However, as the circuit split revealed two years later, that is not the case.

Third-party doctrine and *Carpenter* do not provide clarity, and the voluntary consent concept is difficult for lower courts to apply. The voluntary consent concept is similar to the "knowingly and voluntarily shared" test because, as Kerr explains it, "disclosure to third parties eliminates protection because it implies consent."[159] As we have seen in the circuit courts, judges struggle to apply this sort of test to technology because determining whether a user voluntarily consented is complicated with

154. Carpenter v. United States, 585 U.S. 296, 387 (2018) (Gorsuch, J., dissenting).

155. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 588 (2009).

156. *Id*.

157. Matthew J. Tokson, *The Carpenter Test as a Transformation of Fourth Amendment Law*, 2023 ILL. L. REV. 507, 511.

158. *Id.* at 582.

159. Kerr, *supra* note 155, at 587.

confusing user agreement forms[160] and with the necessity of these applications for daily life.[161] Other courts have also uncovered this problem and questioned how voluntary the location-data-sharing process is.[162] This is because users are often left in the dark about what they are sharing, how much they are sharing, and with whom they are sharing it.[163] Beyond confusion and necessity, consent is also complicated by these applications because some will continue to track your data even if you stop using or delete the application.[164] As one scholar puts it, "Consent to collection, use,

160. United States v. Chatrie, 590 F. Supp. 3d 901, 911 (E.D. Va. 2022) ("No expert could say *exactly* which software pathway Chatrie would have seen when he enabled Location History, nor could Google determine which app he used to turn the service on."), *aff'd*, 107 F.4th 319 (4th Cir. 2024), *and aff'd on reh'g en banc*, 136 F.4th 100 (4th Cir. 2025) (per curiam), *cert. granted*, No. 25-112, 2026 U.S. LEXIS 705 (U.S. Jan. 16, 2026).

161. *See supra* Sections II.B-C; *cf.* Kerr, *supra* note 155, at 588 ("So long as a person knows that they are disclosing information to a third party, their choice to do so is voluntary and the consent valid.").

162. *See, e.g.*, *In re* Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 737 (N.D. Ill. 2020) ("The Court finds it difficult to imagine that users of electronic devices would affirmatively realize, at the time they begin using the device, that they are providing their location information to Google in a way that will result in the government's ability to obtain – easily, quickly and cheaply – their precise geographical location at virtually any point in the history of their use of the device."); Cristina Del Rosso & Carol M. Bast, *Protecting Online Privacy in the Digital Age:* Carpenter v. United States *and the Fourth Amendment's Third-Party Doctrine*, 28 CATH. U. J.L. & TECH. 89, 120-21 (2020).

163. *See supra* note 115.

164. The district court in *Chatrie* described it in this way:

> Once a user opts into Location History, Google is 'always collecting' data and storing *all* of that data in its vast Sensorvault, even 'if the person is not doing anything at all with [his or her] phone.' . . . 'Once enabled, [Google is] now collecting [the user's] location history all the time.' Even if a user enables Location History through an application and later deletes that app, Location History will 'still collect[]' data on the user because Location History is tied to an individual's Google *account*, not to a *specific app.* Thus, after a user opts into the service, Location History tracks a user's location across every *app* and every *device* associated with the user's account.

Chatrie, 590 F. Supp. 3d at 909 (citation modified).

and disclosure of personal data is often not meaningful" because the opt-in process is confusing and not always voluntary.[165]

In developing these arguments, Kerr and Tokson did not have the circuits' decisions to guide their proposals and unfortunately, the circuits' opinions show just how unworkable the doctrine is as it stands and just how unsuccessful a consent and voluntariness approach is. With the knowledge provided by the circuit split, this Note presents a much more workable version of third-party doctrine for location data.

Even one of the main scholarly critiques of *Carpenter* and third-party doctrine also relies heavily on the "knowingly and voluntarily exposed" test and thus fails in practicability considering the circuit courts' decisions. This critique argues for a departure from *Carpenter* and a return to *Katz*, a landmark case where the Court explained that even things accessible to the public may be constitutionally protected as private if a person has a reasonable expectation of privacy in them.[166] For example, Tonja Jacobi and Dustin Stonecipher argue for a return to *Katz* and specifically a test that first looks at whether data is "knowingly exposed" and second looks at whether it is exposed "to the public."[167] They argue that "knowingly exposed" should be "equate[d] with an informed choice" and that courts can look at "contracts and terms of service."[168] However, as the circuit split shows, determining whether something was an informed choice or what a "reasonable person" should have known in the digital age is no easy task, especially with contracts and terms of service.[169] For example, the idea that a user knows what they are sharing comes into question when you examine the prompts users receive. The Google prompt tells users that sharing their location will lead to "app optimization" and does not "reveal the fact that users' locations will be comprehensively stored in a 'Sensorvault,' providing Google the means to access this data and share it with the government."[170] Indeed, the problem of informed consent with contracts and terms of

165. Solove, *supra* note 85, at 1881.

166. Katz v. United States, 389 U.S. 347, 351-52 (1967).

167. Jacobi & Stonecipher, *supra* note 44, at 830.

168. *Id*. at 877.

169. The Fifth Circuit and the original Fourth Circuit reached different conclusions on this issue. *See supra* Section II.B.

170. United States v. Smith, 110 F.4th 817, 835 (5th Cir. 2024), *cert. denied*, No. 24-7237, 2025 U.S. LEXIS 4192 (U.S. Nov. 10, 2025).

service has been widely recognized in the fields of contract law[171] and arbitration.[172] This is likely because very few adults actually read the terms of service they are agreeing to—indeed, users often ignore privacy policies altogether.[173] Yet, even when they do read terms of service users often cannot understand them.[174] For these reasons, this Note's approach does not look at knowledge or informed consent and instead introduces purpose to create a much more workable framework, as explained in the next Part.

III. THE NEW PURPOSE-SENSITIVITY APPROACH

As this Note has shown, third-party doctrine is ill-suited for location data in our technological age. As such, this Note advocates that courts no longer use third-party doctrine for location data as it stands and instead create a new approach that returns to the essence of the Fourth Amendment and this Court's jurisprudence. This new Purpose-Sensitivity approach asks two questions: (1) whether, in sharing their location data with third parties, the user's purpose was to share that information broadly with the public; and (2) whether the location data shared does or could contain sensitive information. This Part explains the test and how to implement it. Part IV defends the test, explaining how it is informed by the circuit courts'

171. *See, e.g.*, Ian Ayres & Alan Schwartz, *The No-Reading Problem in Consumer Contract Law*, STAN. L. REV. 545 (2014); Florencia Marotta-Wurgler, *Will Increased Disclosure Help? Evaluating the Recommendations of the ALI's "Principles of the Law of Software Contracts*," 78 U. CHI. L. REV. 165, 179-81 (2011); Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print? Testing a Law and Economics Approach to Standard Form Contracts* 1 (N.Y.U. Sch. of L. Ctr. for L., Econ. & Org., Working Paper No. 09-40, 2009).

172. *See, e.g.*, Judith Resnik, Stephanie Garlock & Annie Wang, *Collective Preclusion and Inaccessible Arbitration: Data, Non-Disclosure, and Public Knowledge*, 24 LEWIS & CLARK L. REV. 611 (2020).

173. Colleen McClain, Michelle Faverio, Monica Anderson & Eugenie Park, *How Americans View Data Privacy*, PEW RSCH. CTR. (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/ [https://perma.cc/4Y8K-3Z23].

174. Geoffrey A. Fowler, *I Tried to Read All My App Privacy Policies. It Was 1 Million Words*, WASH. POST (May 31, 2022), https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/; Kevin Litman-Navarro, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.*, N.Y. TIMES (June 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.

reasoning, in line with jurisprudence, responsive to critiques, and feasible for the current Court.

A. Prong One: Purposeful, Broad Sharing

As the first step to the Purpose-Sensitivity approach, the Purpose prong asks courts to determine if the user purposefully shared their location information broadly with the greater public. This differs from the third-party doctrine inquiry because there, courts ask whether the information was "knowingly and voluntarily" exposed to a single third party. Instead, the Purpose prong suggests courts focus on if the user's purpose was to share with the broader public, beyond just a third party. To support this approach, this Part first discusses the Supreme Court's precedent that involves determining if something has been shared broadly. Next, it discusses how the criminal legal system already uses purpose and why it is useful here. This Part then proposes factors courts should assess and discusses how these factors are similar to those applied in cases involving location information and data. From there, this Part ends with a brief discussion of hypothetical examples applying this step of the Purpose-Sensitivity approach.

To examine if a user purposefully shared their location information more broadly with the public, courts should rely on prior cases that have balanced whether information was shared broadly with the public. Over time, the Court has determined that just because something may appear public on its face does not mean it is; instead, purpose and privacy may help determine if something is truly public. The Court first looked at sharing with the public in terms of property and location. For example, in *Knotts*, the Court reasoned that surveilling a beeper, or radio transmitter,[175] was an acceptable search because "[t]he governmental surveillance conducted by means of the beeper in this case amounted principally to the following of an automobile on public streets and highways."[176] This helps explain how the Court conceived of "public" versus private. In *Jones*, the Court helped to explain limits on what is considered public when it held that a GPS tracker on a car was a Fourth Amendment–protected search. Justice Sotomayor wrote, "I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone,

175. United States v. Knotts, 460 U.S. 276, 276 (1983) ("A beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver.").

176. *Id.*

disentitled to Fourth Amendment protection."[177] This shift in perspective on tracking car movements in public spaces occurred for a few reasons, but most notable was the influence of *Katz*, a landmark Supreme Court decision, on this determination. In *Katz*, the Court explained that "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[178] Accordingly, the Court recognizes a need to look to the *purpose* of the person being searched. In *Smith v. Maryland*, the Court applied *Katz*'s rationale and determined that a person knew the phone numbers they dialed were shared publicly—not just with the phone company—and even used by others to determine their rates. This is another example of the way the Court has examined who someone has shared their information with and whether the individual shared it publicly. This Note argues that courts should use this same reasoning to determine whether a person purposefully shared their location information with the public more broadly.

As further evidence that courts regularly do this kind of inquiry, the purpose aspect of the Purpose-Sensitivity approach is similar to the purpose requirement for mens rea established by the Model Penal Code. The Model Penal Code defines "acting purposely" as having "an underlying conscious object to act."[179] As the Model Penal Code and its commentary establishes, purpose is preferred to knowledge because it "depend[s] on the actual state of mind of the actor rather than on what a reasonable man in the circumstances would have contemplated."[180] To distinguish purpose from knowledge "[i]t is meaningful to think of the actor's attitude as different if he is simply aware that his conduct is of the required nature or that the prohibited result is practically certain to follow from his conduct."[181]

177. United States v. Jones, 565 U.S. 400, 418 (2012) (Sotomayor, J., dissenting) (first citing Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."); then citing Katz v. United States, 389 U.S. 347, 351-52 (1967) ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.")).

178. *Katz*, 389 U.S. at 351-52.

179. MODEL PENAL CODE § 2.01(2)(a) (A.L.I., Proposed Official Draft 1962).

180. *Id.*

181. *Id.* § 2.02 cmt. at 233.

This distinction will assist courts in avoiding the challenges of a knowing standard based on reasonableness. One of the most critiqued aspects of third-party doctrine and proposed substitutes is that they require courts to do a reasonableness analysis of what a user should have known or actually knew.[182] Determining what someone knew or should have known has proven quite difficult for courts, as evidenced by the divergence in opinion on this issue by the circuits. For example, the Fourth and Fifth Circuits reached different conclusions, and the *Carpenter* Court declined to extend third-party doctrine in part because of the difficulty in applying the "knowingly and voluntarily shared" aspect to a cell phone.[183] By focusing on purpose, courts will be able to better apply the Purpose-Sensitivity approach to technology where inferring knowing and voluntary choice is difficult because the act is almost required or forced upon a person. Purpose is also well established in criminal law and as such is a clearer inquiry than knowledge.

In determining if a user purposefully shares their location information *with the public* more broadly, courts would examine two factors. First, courts should examine whether the user purposefully shared their location information with more than just a third-party conduit, like Google. For example, when someone uses Google Maps, they purposefully share their location with Google, but they do not purposefully share it with anyone beyond Google. This factor would rely on the mens rea purpose requirement in criminal law, meaning that it would consider whether the user had the conscious intent to act and cause the result. Second, courts should examine if the user had the purpose to share the location information with the public more broadly, beyond the third party, or if they intended to keep it private. For example, when someone uses Find My Friends, they are purposefully sharing their location data with more than just Apple; they are sharing it

182. Scholars and courts alike are critical of the reasonableness test. For example, Justice Scalia said that the expectations society has of reasonableness "unsurprisingly . . . bear an uncanny resemblance to those . . . that this Court considers reasonable." Minnesota v. Carter, 525 U.S. 83, 97 (1998). The reasonableness test is even more difficult as applied to technology. *See supra* note 85.

183. Carpenter v. United States, 585 U.S. 296, 298 (2018) ("Cell phone location information is not truly 'shared' as the term is normally understood. First, cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society. Second, a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the user's part beyond powering up." (citation omitted) (citing Riley v. California, 573 U.S. 373, 385 (2014))).

with their selected friends too. Or when someone shares something on a public social media account, they are sharing it with more than the social media company, arguably with the general public too. This part of the analysis would rely on mens rea purpose and the Supreme Court's prior cases that examined what is public and what is private, like *Jones* and *Katz*. By examining these factors, lower courts can rely on the Supreme Court's previous reasoning to determine if a user purposefully shared their information with the broader public.

To explain the proposed reasoning behind this prong, some brief and very simplified hypotheticals are useful. Take, for example, a person who has a public Instagram account and posts multiple photos with location tags. The government then requests the geotag location data of this user from these images to build a case against this person in a criminal action. In this case, the court could look at the information and see that (1) the person purposefully shared the information with more than just Instagram, and (2) the person likely knew and purposefully shared these pictures with the public because their Instagram was public. Here, the user *purposefully* shared the information with the public more generally.

As another example, take someone with a Snapchat account who shares their location with their friends via Snap Map. They have selected only a subset of their friends on Snapchat to have access to their location from Snap Map. The app catalogues their location continuously but only those friends who have access can see it. The government subpoenas Snapchat for the Snap Map location of all the users in a certain area over a certain time, hoping they can find who was present at a robbery. In going through the factors the court may find (1) the user purposefully shared their location information with more than just Snapchat—they had chosen the friends who would see it as well, and (2) the user did not know or purposefully share the information with the public more broadly—they chose from a limited group of their friends an even more limited subset to share their Snap Map location with. The user's purpose was clearly to limit who could access this information.

These hypotheticals are fairly clear-cut and oversimplified.[184] Courts will likely face more challenging scenarios, like a Facebook user with only

184. These hypotheticals and those in Section III.B use examples like Yelp, Snapchat, and Instagram, which may not seem necessary to participate in daily life, but there are many apps that arguably are, like navigation apps, weather apps, and rideshare apps, which all collect location data. *See supra* note 5. As explained in Section III.C, the new Purpose-Sensitivity test does not consider whether an app is necessary for daily life, because such

twelve friends but a public account, who posts updates with their location multiple times a day. However, courts are well equipped to make determinations with these factors by relying on the various tools outlined above. Additionally, part of the adversarial process is a lack of bright-line rules where parties must make their best arguments and courts must make fact-based determinations.

B. Prong Two: Sensitivity

As the second step to the test, courts should determine whether the location data shared does or could contain sensitive information. In doing so, courts would look at the facts of each case and determine whether the information obtained by the government revealed or could have revealed private information. This is similar to the inquiry courts make in Fourth Amendment cases that do not involve third parties, where courts address whether a person has a reasonable expectation of privacy in something based on sensitivity. This Section first outlines the Court's precedent on determining what is sensitive and private. From there this Section shows examples of how the Court has thought about sensitivity in location and data cases. This Section then concludes with a discussion of the specific factors courts should and have considered to determine if location information is sensitive or private.

In order to conduct this step, courts would need to rely on precedent that involves determining if something is regarded as private under the Fourth Amendment. As expanded on in Part IV, the guiding test on privacy is largely derived from *Katz v. United States*.[185] In *Katz*, Justice Harlan put forth a two-prong test for privacy, which first examines whether a person has an actual expectation of privacy and second whether that expectation is one that society would recognize as reasonable.[186] In *Katz*, the Court primarily focused on the location and physical context of the search as opposed to the actual content of what was being searched.[187] However, courts have built upon this and continually applied *Katz* to determine what

considerations are not in line with the Fourth Amendment and with third-party doctrine, as it was initially conceived.

185. 389 U.S. 347 (1967).

186. *Id.* at 361 (Harlan, J., concurring).

187. *Id*. at 350-52.

is private in various settings. Relying on *Katz*, Courts have also created other benchmarks for determining what is private.[188]

In *Jones*, the concurrences set out examples for determining what is private and sensitive. Justice Sotomayor wrote that a GPS search violated privacy because it creates "an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[189] There is also extensive language in *Jones* on what the Justices understand to be private and sensitive for the Fourth Amendment.[190] These cases provide examples of how the Court has reasoned through what is an intrusion of privacy.

Importantly, the Court has recognized that even if the government's particular use does not infringe on a private and sensitive matter, there are still Fourth Amendment limits if the government's actions *could* have revealed something private or sensitive. In making these determinations, the Court has relied on the purpose of the Fourth Amendment to limit government intrusion. For example, the Court has explained that "[t]he Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained."[191] Explaining why thermal imaging to search a home is unconstitutional, the Court said that "[l]imiting the prohibition of thermal imaging to 'intimate details' would not only be wrong in principle; it would be impractical in application, failing to provide 'a workable accommodation between the needs of law enforcement and the interests protected by the Fourth Amendment.'"[192] When thinking about what is private and sensitive in

188. For example, see *infra* notes 190 and 265 and accompanying text.

189. Carpenter v. United States, 585 U.S. 296, 311 (2018) (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

190. *Jones*, 565 U.S. at 415 ("In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention. GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. *See, e.g.*, *People* v. *Weaver*, 12 N. Y. 3d 433, 441-442 (2009) ('Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on')." (citation modified)).

191. Kyllo v. United States, 533 U.S. 27, 37 (2001).

192. *Id.* at 38 (citing Oliver v. United States, 466 U.S. 170, 181 (1984)).

terms of a search, the Court has made it clear that paying attention to the powers and scope of the search to uncover intimate details is just as important as whether the search actually revealed those private details. This balancing test is precisely why the Sensitivity prong of the Purpose-Sensitivity approach requires that courts consider not only the sensitivity of the information revealed, but also the possibility that something sensitive could have been revealed.

The Court's precedent provides clear guidelines for determining whether information is private and sensitive under the Sensitivity prong. These guidelines provide three factors courts should examine for the Sensitivity prong. First, courts should look at whether the individual had a reasonable expectation of privacy in the information. To do this, they can rely on *Katz* and other precedent that examines privacy. The second factor is the intrusiveness and breadth of the search. For this factor, courts can rely on *Carpenter*. The third factor is whether the government did or could have revealed something that was private. This factor would use the Court's precedent that discusses the ability of a search to reveal private information.

Some hypotheticals can motivate understanding of this prong. Consider a case where a robbery occurred at a restaurant. The restaurant is popular on Yelp, so the government requests the location information from Yelp of all the users who it pinged at the restaurant on the night of the robbery. The government only wants the information regarding this one ping; they do not want any other location information. From this location information, they find a suspect and use this information to charge them with the crime. For the factors, this Note suggests the court would first look at whether the individual had a reasonable expectation of privacy. The court may determine that since the government is only requesting information from a public space, the restaurant, there may not be a reasonable expectation of privacy. For the second factor, intrusiveness and breadth, the court may decide that if the government wants only one location at a limited time, then it is not overbroad or intrusive. The third factor, whether the government did or could have revealed something private, is a bit more complicated. The restaurant is public, but perhaps through location data it could be revealed that someone is on a date and having an affair. Relying on precedent, the court could determine that since it was only revealing the one instance and not a catalogue, the search did not and likely could not reveal something private. As such, this request likely survives the Sensitivity prong.

Of course, these two prongs would be taken together and not individually. This Note acknowledges that both of these prongs and this test are not without their shortcomings, which are addressed in Section IV.D.

However, as is expanded upon in the next Part, this test would help align courts with the Supreme Court's jurisprudence and the text and Framers' intent of the Fourth Amendment to restrict the government's ability to obtain information intended to be kept private.

C. Informed by *Chatrie* and *Smith*

The proposed test is both responsive to and informed by the decisions made in the lower courts. As such, it helps to clear up the confusion of lower courts while also considering the precedent set in these circuits. As previously discussed, the circuit courts primarily disagreed over the application of *Carpenter*. The Fourth Circuit in the original *Chatrie* decision thought the application of *Carpenter* was clear-cut, that third-party doctrine applied because the information sought did not implicate privacy concerns, and that Chatrie voluntarily exposed the information to a third party.[193] In the subsequent en banc decision, the Fourth Circuit could not reach a decision about how to apply *Carpente*r and whether third-party doctrine applied and instead upheld the lower court's decision, which also left the question of *Carpenter*'s third-party doctrine open and held that the good faith exception applied.[194] The Fifth Circuit majority in *Smith* found that location data is inherently private and cited concerns from *Carpenter* to reach this conclusion.[195] The court also determined that Smith did not "knowingly or voluntarily expose" his information because people must trust third parties with their information in the digital age.[196] As such, the circuit courts largely disagreed over what makes something sensitive and private and what is required for sharing to be "knowing and voluntary."[197]

193. United States v. Chatrie, 107 F.4th 319, 331 (4th Cir. 2024), *aff'd*, 107 F.4th 319 (4th Cir. 2024), *and aff'd on reh'g en banc*, 136 F.4th 100 (4th Cir. 2025) (per curiam), *cert. granted*, No. 25-112, 2026 U.S. LEXIS 705 (U.S. Jan. 16, 2026).

194. United States v. Chatrie, 590 F. Supp. 3d 901, 941 (E.D. Va. 2022), *aff'd*, 107 F.4th 319 (4th Cir. 2024), *and aff'd on reh'g en banc*, 136 F.4th 100 (4th Cir. 2025) (per curiam), *cert. granted*, No. 25-112, 2026 U.S. LEXIS 705 (U.S. Jan. 16, 2026).

195. United States v. Smith, 110 F.4th 817, 832-33 (5th Cir. 2024), *cert. denied*, No. 24-7237, 2025 U.S. LEXIS 4192 (U.S. Nov. 10, 2025).

196. *Id*. at 835-36.

197. *Compare id.* at 833 (explaining that location tracking "can easily follow an individual into areas normally considered some of the most private and intimate"), *with Chatrie*, 107 F.4th at 323 ("Location History's power should

The original circuit courts' reasoning informs the Purpose-Sensitivity approach. The Purpose prong is similar to the reasoning in the original *Chatrie* dissent. There, Judge Wynn wrote, "The explosive growth of the usage of new technologies, such as smartphones, illustrates a certain level of comfort among the American populace in entrusting personal information to technology companies like Google."[198] However, "that does not mean such trust extends to the State or that the American populace has ceded its reasonable expectation of privacy in that information."[199] Instead, "[i]t is a grave misjudgment to conflate an individual's limited disclosure to Google with an open invitation to the State."[200] This demonstrates the type of analysis that this Note suggests courts do in determining if information was purposefully shared broadly.

The Sensitivity prong would also look similar to the analysis in the original *Chatrie* dissent that examined both the depth and breadth of the intrusion, and the intimacy of the information revealed. In discussing the depth and breadth, the dissent focused in on a few different factors. Importantly, it looked at how location data can provide a complete look at someone's movements in ways that create deep privacy concerns.[201] To make these conclusions, the dissent relied on the accuracy and precision of location tracking.[202] Additionally, the dissent focused on the fact that location data can intrude upon protected spaces "that could not otherwise have been obtained without physical intrusion into a constitutionally protected area."[203] Similarly, the intimacy prong in the original *Chatrie* dissent focuses on the personal and revealing nature of the information that location data can reveal. The dissent asserts that the length of tracking does not matter because even in a short amount of time location data can provide

not be exaggerated. In the end, it is only an estimate of a device's location."); *compare Smith*, 110 F.4th at 835-36 ("[E]lectronic opt-in processes are hardly informed and, in many instances, may not even be voluntary."), *with Chatrie*, 107 F.4th at 331 (finding that sharing Location History with Google is knowing and voluntary because the user "affirmatively" opts in to sharing, and receives "ample notice about the nature of this setting").

198. *Chatrie*, 107 F.4th at 360 (Wynn, J., dissenting).

199. *Id.*

200. *Id.*

201. *Id*. at 348-51.

202. *Id*. at 350.

203. *Id*. at 350 (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

intimate associations by revealing travel to private and protected spaces like homes, doctor's offices, and religious institutions.[204]

Additionally, the Sensitivity prong is similar to the analysis done by the original majority in *Chatrie*, where the court examined the nature of the information sought. However, the court there intertwined the nature of the information sought and the fact that it was "knowingly and voluntarily exposed" to a third party to determine that it was not sensitive or private.[205] The court therefore allowed the fact that Chatrie had shared the information with a third party to color its analysis of whether the information was sensitive or private. Meaning because the privacy analysis was done within the confines of the current flawed third-party doctrine, the court used the fact that Chatrie had shared the information with a third party as evidence that it was not private. The Purpose-Sensitivity approach avoids this conflation by excluding from the Sensitivity prong whether or not the information was shared with a third party. As this Note has shown, justices and scholars have recognized that sharing data is required to participate in daily life, and just because it is shared with a third party does not mean that it is not private or sensitive.

By pulling from the reasoning and rationale of the circuit courts, the Purpose-Sensitivity approach is responsive to them. Specifically, the Purpose prong responds to the major confusion over the "knowing and voluntary" test, confusion created by the fact that sharing with third parties is required to participate in modern life and often involves some hidden clause in a user agreement. However, by broadening the test to determining if a user's purpose was to share with the broad public, the test no longer looks at hidden clauses and gets more to the root of the act of sharing. This means that judges will no longer need to quibble over how much a user knew, how informative the consent process was, or if using the app was a necessity of daily life. As explained in Section IV.B, this is also in line with the Fourth Amendment and precedent which looked at the difference between private and public.

By better balancing third-party doctrine with other privacy doctrine, the Sensitivity prong of the proposed test is also responsive to the confusion over how to apply *Carpenter* and what factors *Carpenter* considered for extending third-party doctrine. This is because the circuit courts did not understand how to balance the third-party doctrine test with prior doctrine about privacy. Meaning, they considered that the user had shared the information with a third party when they determined whether it was

204. *Id*. at 350, 370.

205. *Id*. at 330-32.

private, which of course skews the decision. The proposed approach, in contrast, does not consider that information was shared with a third party when determining if it was private. Additionally, the proposed test provides clear guidance for making privacy determinations, which the lower courts struggled to do. For example, the Fourth Circuit thought that location data from a short time frame was less likely to implicate privacy concerns, whereas the Fifth Circuit thought that *Carpenter* instructed it to consider other factors outside of time in determining privacy.[206] The Purpose-Sensitivity approach clarifies what factors are important by pulling from not only *Carpenter*, but also *Katz*, *Smith*, *Miller*, and the original intent of the Fourth Amendment. As a result, the Sensitivity prong accounts for the factors that the lower courts found instructive while also providing a clearer path forward.

The Purpose-Sensitivity approach also responds to the divergence between the original dissent and majority in *Chatrie*. There, the judges disagreed over what test *Carpenter* set out and what "knowingly and voluntarily" exposed truly meant. The majority decided that *Carpenter* required the court to ask if the information sought by the government had limited privacy concerns, to which the majority said yes. Conversely, the dissent determined that *Carpenter* set out five factors to address in totality. These differences highlight the difficulty the lower courts have in applying *Carpenter*, a difficulty the proposed test overcomes.

IV. GROUNDING AND DEFENDING THE PURPOSE-SENSITIVITY APPROACH

The new Purpose-Sensitivity approach is both appropriate and implementable because it is in line with precedent, consistent with the Fourth Amendment, and responsive to concerns with third-party doctrine. Specifically, this new Purpose-Sensitivity approach returns third-party doctrine back to the Court's intent in *Smith* and *Miller*. It also follows from the Supreme Court's other Fourth Amendment precedent like *Katz* and *Carpenter*. It connects the holdings from these four cases to bring third-party doctrine back in line with a standard that fits the technological era. Accordingly, implementing the Purpose-Sensitivity approach does not require overruling any precedent. This adapts the Fourth Amendment to the current era, while remaining true to the Framers' intent and the Court's application. Lastly, it is informed by the shortcomings of the third-party doctrine and its critiques.

206. *See supra* Section II.B.

A. Guided by Precedent

This Section explains how the Purpose-Sensitivity approach follows from the precedent and is thus highly implementable. Specifically, the approach is in line with the cases that created third-party doctrine as well as two other landmark Fourth Amendment cases, *Katz* and *Carpenter*. Beyond that, it marries these cases together in a way that brings third-party doctrine into the modern era, without overturning any precedent. As such, the test is congruous and practical for the current Court and jurisprudential landscape.

1. Third-Party Doctrine: *Smith* and *Miller*

This Note argues that the Purpose-Sensitivity test is in line with *Smith* and *Miller*, restoring third-party doctrine's original purpose as applied to location data. Third-party doctrine was developed with a focus on privacy and the expectation of privacy in sensitive documents. As such, while location data was not at issue in either *Smith* or *Miller*, implementing the Purpose-Sensitivity test would not require overturning either. The approach, then, is highly practicable as it would not necessitate overruling any precedent.

The Purpose-Sensitivity approach returns third-party doctrine to its privacy-protecting roots. As this Note has shown, third-party doctrine, as it stands, does not meet this purpose. Instead, third-party doctrine means that courts do not even examine the privacy of what was shared and instead decide that if something was shared with a third party, it is necessarily not private. Conversely, by examining the range of people that the user purposefully shared their information with, this Note's approach is in line with the original intent of the Court. For example, in *Smith* and *Miller*, the Court determined that the defendants knowingly and purposefully shared their information, whether it was with bank workers during transactions or phone companies while transferring calls. The users chose to share their information and relied on others knowing it and using it, meaning it was part of the user's purpose to share their information. The knowledge inquiry in *Smith* and *Miller* implicitly looked at purpose as well. However, as applied today, third-party doctrine does not involve examining a user's purpose. Instead, courts look at if the user "knowingly and voluntarily" exposed the information. But as explained, with location data, it is often difficult for courts to apply the "knowingly and voluntarily" exposed test, as evidenced by recent lower-court decisions. The Purpose-Sensitivity approach looks at the purpose of the user instead, as *Smith* and *Miller* did implicitly.

Another aspect of the third-party doctrine was the nature of the information sought and whether it implicated privacy or was sensitive, which the Purpose-Sensitivity approach also considers. In *Smith* and *Miller*, the Court examined whether the information shared implicated privacy concerns and determined that it did not. The Court ruled that the dialed phone numbers and bank information were not of a private nature and were not confidential. The nonsensitive nature of the information informed the Court's development and application of third-party doctrine. With location data, privacy implications are more pressing and evident because location data can provide an intimate and chronicled look into someone's life. However, currently under third-party doctrine, courts do not look at the privacy implications and instead only look at if the information was "knowingly and voluntarily" exposed. This strays from *Smith* and *Miller*, which used privacy in their reasoning. For example, in *Miller*, the Court determined that there were limited privacy concerns because the information sought was "not confidential communications but negotiable instruments to be used in commercial transactions" and "exposed to [bank] employees in the ordinary course of business."[207] And in *Smith* the Court used privacy in its reasoning and said that it "doubt[s] that people in general entertain any actual expectation of privacy in the numbers they dial."[208] This privacy inquiry is completely lost in the modern application of third-party doctrine to location data. In order to be true to *Smith* and *Miller*, the second prong of the Purpose-Sensitivity approach is focused on sensitivity. The Purpose-Sensitivity test is thus aligned with the original intent of third-party doctrine, and normatively and practically defensible.

2. *Katz*

Besides third-party doctrine, another line of inquiry for Fourth Amendment searches is the *Katz* test.[209] The Purpose-Sensitivity approach flows from *Katz* while responding to its critiques. In *Katz*, the Court explained that even things accessible to the public may be constitutionally protected as private if a person has a reasonable expectation of privacy in them.[210] Central to the holding in *Katz* was a person's expectation of privacy—a key factor in the Purpose-Sensitivity approach. In *Katz*, the Court

207. United States v. Miller, 425 U.S. 435, 442 (1976).

208. Smith v. Maryland, 442 U.S. 735, 742 (1979).

209. Katz v. United States, 389 U.S. 347, 347 (1967).

210. *Id.* at 351-352.

determined that "[t]he Fourth Amendment protects people, not places," and in doing so, expanded the protections it provides.[211] Importantly, *Katz* also introduced the idea of a "reasonable" expectation of privacy, even in areas where the public may have access.[212] The Purpose-Sensitivity approach moves us back to this understanding of the Fourth Amendment, centered on privacy, which is one that the Court continues to rely on today.[213]

Conversely, current third-party doctrine departs from *Katz* because currently, if someone shares something with a third party, that is the end of the inquiry. A court does not consider a person's expectation of privacy or the sensitivity of the information shared. By using the Purpose-Sensitivity approach and inquiring whether the user purposefully shared location information broadly beyond a third party, courts would perform a tweaked version of the *Katz* reasonableness test. By looking at the sensitivity of what was purposefully shared, courts can answer the question of whether the information was "expose[d] to the public" or whether the user intended "to preserve [it] as private."[214]

Beyond being aligned with *Katz*, the Purpose-Sensitivity approach responds to criticism of *Katz*. One common critique of *Katz* is that its reasonableness test is unclear and often too subjective.[215] This often derives from the "knowing" requirement and the difficulty courts have in determining what a "reasonable person" should have known. The proposed approach responds to this critique because it uses "purpose" instead of "knowing" and does not rely on what a reasonable person would or should know. Instead of looking at an imagined "reasonable person," it looks at what the actual person's purpose was.[216] Accordingly, the Purpose-Sensitivity approach adopts and adapts *Katz*, a test currently used by the Court, and makes the analysis even more implementable.

---

211. *Id*. at 351.

212. *Id.*

213. Carpenter v. United States, 585 U.S. 296, 303 (2018) ("The 'basic purpose of this Amendment,' our cases have recognized, 'is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.'" (quoting Camara v. Mun. Ct. of S.F., 387 U.S. 523, 528 (1967))).

214. *Katz*, 389 U.S. at 351.

215. Minnesota v. Carter, 525 U.S. 83, 97 (1998).

216. MODEL PENAL CODE § 2.02 cmt. at 235-36 (A.L.I., Proposed Official Draft 1962) (explaining that the "distinction between purpose and knowledge" is that purpose "depend[s] on the actual state of mind of the actor rather than on what a reasonable man in the circumstances would have contemplated").

3. *Carpenter*

The Purpose-Sensitivity approach also flows from *Carpenter*. The Court's decision not to extend third-party doctrine to cell site location information shows exactly why third-party doctrine should not be applied to location data and why the Purpose-Sensitivity approach is a better replacement for the current third-party doctrine. As previously discussed, the *Carpenter* Court declined to extend third-party doctrine because of the nature of information sought and because of concerns with determining if the information was "knowingly and voluntarily" shared.

Location data catalogues a person's whereabouts and movements with questionable knowledge and consent, highlighting how third-party doctrine is ill-suited for location data. Conversely, the Purpose-Sensitivity approach suggests that a court should not overlook the privacy interests at stake just because a user shares their information with a third party. Instead it suggests that courts should determine if the information shared is private and sensitive. As such, the Purpose-Sensitivity approach follows from *Carpenter* by examining and appropriately weighing the privacy and sensitivity of the information sought, without indiscriminately applying third-party doctrine anytime information is shared with a third party. The Purpose-Sensitivity approach also addresses concerns with knowledge and voluntariness by examining whether users purposefully shared the information more broadly and made it public. By focusing on purpose, the Purpose prong avoids the confusion of applying "knowing and voluntary" to complex user agreements and technology that is almost required for daily life. The two prongs, taken together, will help courts remain true to the real concerns of the Justices without getting caught up in how informed the user was about where their data was going and who could access it. This would in turn bring lower courts in line with the decision in *Carpenter*, while saving the courts the time and resources it takes to determine a user's knowledge and whether sharing the information was voluntary.

4. Lessons from Precedent

The new Purpose-Sensitivity approach flows directly from precedent. Specifically, it is in line with the intent of third-party doctrine because it addresses both the nature of the information sought and reasonable expectation of privacy. It also follows from both *Katz* and *Carpenter*. Importantly though, it combines *Katz* and *Carpenter* to help the Court adopt a Fourth Amendment doctrine standard that fits our technological era and remains true to the Fourth Amendment.

B. Rooted in the Fourth Amendment

The proposed Purpose-Sensitivity approach is both aligned with the Fourth Amendment's text and the Framers' intent. It also draws from the Court's recent interpretation and application of the Fourth Amendment, making it practical under the current Court's predilection for originalism.

1. Text and Founders' Intent

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[217] The Framers wrote the Fourth Amendment to ensure that the government would have limits on its powers when it came to searching and seizing.[218] This concern came from the Framers' experience prior to the American Revolution when British subjects were faced with writs of assistance and general warrants, which were both used by British officers to search a person's home, papers, or effects.[219] Frustration and outrage with these searches contributed to the American Revolution.[220] Understanding the Fourth Amendment in its historical context illuminates that it is meant to be a restriction on the government's power, which this Court has recognized.[221] This is evident through the text of the amendment as well.

The text says that it is "a right of the people" to be free from "unreasonable searches."[222] By declaring it a right of the people, the Framers spoke to "the purpose of the Fourth Amendment," which "was to protect the people of the United States against arbitrary action by their own Government."[223] In order to protect the rights of the people against unreasonable searches, courts must do more than consider whether the

217. U.S. CONST. amend. IV.

218. Riley v. California, 573 U.S. 373, 403 (2014).

219. *Id*.

220. *Id*.

221. *See infra* Section IV.B.2.

222. U.S. CONST. amend. IV.

223. United States v. Verdugo-Urquidez, 494 U.S. 259, 266 (1990); United States v. Jones, 565 U.S. 400, 416-17 (2012) (Sotomayor, J., concurring) (referencing "the Fourth Amendment's goal to curb arbitrary exercises of police power and prevent 'a too permeating police surveillance'" (quoting United States v. Di Re, 332 U.S. 581, 595 (1948))).

information was shared with a third party. Instead, courts must consider how the government obtained the information and the effect that has on the privacy and security of the people. Current third-party doctrine as applied to location data strays from the Framers' intent and the original text of the Fourth Amendment. The proposed approach conforms to both by considering whether the information was broadly shared in a way that allowed the government to obtain it and whether the information obtained implicates privacy concerns.

2. The Court's Application of the Fourth Amendment

In applying the Fourth Amendment, the Court has focused on remaining true to the Framers' intent,[224] which the Purpose-Sensitivity test does. Specifically, the Court has applied the Fourth Amendment "to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."[225] To do this, the Court has kept "Founding-era understandings in mind when applying the Fourth Amendment to innovations in surveillance tools."[226] And "[a]s technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"[227] This reasoning highlights how adhering to the Fourth Amendment, while addressing technological advancements, is especially important for the Justices. Because third-party doctrine blunts Fourth Amendment protections anytime a third party is involved, it limits courts' ability to stay true to the Fourth Amendment. It stops the analysis after a court determines that a user "knowingly and voluntarily" exposed their information to a third party. It also prohibits courts from applying the Fourth Amendment to a new technological era where most things are shared with third parties, especially location data. As such, third-party

224. This approach is relatively new, meaning it is a departure from the Warren and Burger Courts. However, as the Court has become increasingly originalist, this is now the Court's de facto approach. For discussion on the Court's transition to Fourth Amendment originalism, see generally David A. Sklansky, *The Fourth Amendment and Common Law*, 100 COLUM. L. REV. 1739 (2000).

225. Camara v. Mun. Ct. of S.F., 387 U.S. 523, 528 (1967).

226. Carpenter v. United States, 585 U.S. 296, 305 (2018).

227. *Id.* (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

doctrine as applied to location data is not in line with the Court's aims regarding the Fourth Amendment.

The guideposts created by the Supreme Court for Fourth Amendment doctrine also illuminate the Court's intentions, and how the Purpose-Sensitivity approach is responsive. The guideposts, as defined by the Court, are informed by the history and intent of the Fourth Amendment.[228] "First, that the Amendment seeks to secure 'the privacies of life' against 'arbitrary power.'"[229] Second, and relatedly, that a central aim of the Framers was "to place obstacles in the way of a too permeating police surveillance."[230] These guideposts reveal the Court's intentions with the Fourth Amendment and show how third-party doctrine, as applied to location data, has drifted from that intent. Conversely, the Purpose-Sensitivity approach adheres to these guideposts, allowing courts to actually consider the Fourth Amendment for location data, instead of stopping analysis at whether something was shared with a third party.

C. Responsive to Concerns with Third-Party Doctrine

The Purpose-Sensitivity approach also responds to the many concerns with third-party doctrine from both inside and outside the Court, amongst legal scholars and practitioners.

1. The Supreme Court

The Court has expressed concern over technological advancements eroding the protections of the Fourth Amendment. This concern was expressed as early as 1928 by Justice Brandeis who said that as "[s]ubtler and more far-reaching means of invading privacy have become available to the Government" the Court must guarantee that the "progress of science" does not winnow away Fourth Amendment protections.[231] This concern rang even truer for the Justices in *Carpenter*. Justice Gorsuch, for example, said:

> What's left of the Fourth Amendment? Today we use the Internet to do most everything. Smartphones make it easy to keep a calendar,

228. *Id.* at 305 (citing Carroll v. United States, 267 U.S. 132, 149 (1925)).

229. *Id.* (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

230. *Id.* (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

231. Olmstead v. United States, 277 U.S. 438, 473-74 (1928).

> correspond with friends, make calls, conduct banking, and even watch the game. Countless Internet companies maintain records about us and, increasingly, for us. Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers. Smith and Miller teach that the police can review all of this material, on the theory that no one reasonably expects any of it will be kept private. But no one believes that, if they ever did.[232]

This quote perfectly explains the faults of third-party doctrine in the technological era. In *Carpenter*, the technology companies attested that "all digital technology transmits user information to various service providers. . . . Those transmissions are an unavoidable condition of using digital technology."[233] Therefore, if courts continue to rely on third-party doctrine, they will inevitably remove protections from a myriad of things that would typically have Fourth Amendment protections.

Beyond general technological concerns, the Court has expressed specific qualms with surveillance and location data. Specifically, the Court has been concerned with expanding government surveillance capabilities. This concern can be seen through the Court's emphasis on maintaining the Framers' intent of the Fourth Amendment to safeguard privacy.[234] The Court expressed this concern in *Carpenter* when it said that "this tool risks government encroachment of the sort the Framers, 'after consulting the lessons of history,' drafted the Fourth Amendment to prevent."[235] The Justices have become concerned with the way technology, and specifically third-party doctrine, have moved beyond the Framers' intent.

By amending third-party doctrine with the Purpose-Sensitivity approach for location data, courts can return to the essence of the Fourth Amendment and not disregard its guarantees simply because the world has advanced. Technology has improved in such a way that people share almost everything with a third party. As such, if courts apply third-party doctrine indiscriminately, Fourth Amendment protections will soon have no reach. This approach responds to the calls from the Court to ensure that even as the world progresses, Fourth Amendment protections are not entirely

232. *Carpenter*, 585 U.S. at 387 (Gorsuch, J., dissenting).

233. Brief for Technology Companies as Amici Curiae in Support of Neither Party at 18, Carpenter v. United States, 585 U.S. 296 (2018) (No. 16-402), 2017 WL 3530959.

234. *See supra* Section IV.B.

235. *Carpenter*, 585 U.S. at 309.

disregarded simply because a third party has access to our most private information, specifically our location data.

2. Legal Scholars and Practitioners

As was discussed in Part II, the problems with current third-party doctrine and *Carpenter* have been recognized by various scholars. The Purpose-Sensitivity approach responds to the concerns from scholars and practitioners. At the same time, it offers a new and unique solution to the problem. The scholarly critiques can be narrowed down to three main proposals: (1) third-party doctrine is an imperfect but viable doctrine; (2) third-party doctrine should be eliminated entirely; and (3) it should remain, but fundamentally change and move away from *Carpenter*.

As previously discussed, one of the more vocal defenders of third-party doctrine is Orin Kerr. He puts forth two primary arguments: (1) third-party doctrine is necessary to prevent criminals from taking advantage of new technologies to hide their illegal activities; and (2) it helps to protect the clarity of Fourth Amendment rules.[236] Kerr also asserts that the two main criticisms of the doctrine—that it is awkward and unworkable and that it gives the government too much power—are weak.[237] In particular, he argues that third-party doctrine should be understood as a consent doctrine and that "[t]hird-party disclosure eliminates privacy because the target voluntarily consents to the disclosure."[238] With this understanding, he finds, it is clear that third-party doctrine is workable and does not give the government too much power beyond that consented to by the user.[239]

These arguments are unconvincing for three reasons. First, they are not well grounded within Fourth Amendment precedent. As this Note has previously discussed, Justices have expressed real concerns with third-party doctrine eroding the Framers' intent for the Fourth Amendment. The Justices have focused on maintaining this protection through their precedent. However, Kerr's proposal places more weight and value on security and crime deterrence because it disregards the privacy of the general public in order to find one law breaker.[240] As this Note has shown,

236. Kerr, *supra* note 155, at 566.

237. *Id.* at 587.

238. *Id*. at 588.

239. *Id*.

240. *Compare id.* (asserting that "a rational actor bent on criminal conduct will use as many third-party services as he can to avoid detection"), *with* Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and*

the Court has made clear that the Fourth Amendment protects the privacy of individuals and does not favor security over this right.[241]

Second, they are inconsistent with the Framers' understanding of and intent for the Fourth Amendment. As previously discussed, the intent of the Fourth Amendment was to deter government overreach.[242] The Court has repeatedly stated the importance of staying in line with the Framers' intent and protecting the public from government intrusion.[243] However, Kerr's assessment argues that it is more important to prevent criminals from taking advantage of technology to commit crimes.[244] By prioritizing crime prevention, Kerr largely disregards the intent of the Fourth Amendment as outlined by the Framers and the Court.

Third, as discussed in Part II, the consent concept has proven to be unworkable and difficult, and it strays from Fourth Amendment jurisprudence. Kerr's consent concept is similar to the "knowingly and voluntarily shared" test that circuit courts have already struggled to apply to technology.[245] This is because determining whether a user consented is complicated by confusing user agreement forms,[246] unclear use of the data by third parties,[247] and with the necessity of these applications for daily

---

Kerr, 24 BERKELEY TECH. L.J. 1239, 1241 (2009) (arguing that since "the technologies left exposed by third-party doctrine are not exclusively deployed for illicit purposes, failing to protect them generates negative externalities (by dissuading innocent, desirable conduct)"). *See also* Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 45 (2011) (expressing skepticism towards the argument that third-party doctrine is appropriate to prevent "savvy wrongdoers" from hiding criminal activity).

241. Olmstead v. United States, 277 U.S. 438, 479 (1928) ("[I]t is better that a few criminals escape than that the privacies of life of all the people be exposed to the agents of the government.") (Brandeis, J., dissenting).

242. *See supra* Section IV.B.2.

243. *Id.*

244. *See supra* note 240 and accompanying text.

245. United States v. Chatrie, 590 F. Supp. 3d 901, 911 (E.D. Va. 2022) (noting that neither expert nor Google could say *exactly* which software pathway Chatrie would have seen when he enabled Location History and which app he used to turn the service on), *aff'd*, 107 F.4th 319 (4th Cir. 2024), *and aff'd on reh'g en banc*, 136 F.4th 100 (4th Cir. 2025) (per curiam), *cert. granted*, No. 25-112, 2026 U.S. LEXIS 705 (U.S. Jan. 16, 2026).

246. *Id.*

247. *See supra* note 150.

life.[248] As opposed to examining expectations of privacy, Kerr argues for a consent-based application of third-party doctrine. This is counter to Fourth Amendment jurisprudence, which values privacy and individuals having a reasonable expectation of privacy.

Other scholars argue that we should do away with third-party doctrine entirely.[249] This approach is often grounded in a belief that it is entirely incompatible with the digital age. These scholars assert that third-party doctrine was created in an age when technology was rudimentary, so it is impossible to apply it and adapt it to the digital age.[250] This argument has strength, especially given the lack of guidance from the Supreme Court, and the difficulty the lower courts have in applying third-party doctrine to technology. However, the proposal is unpersuasive for two reasons.

First, it is impractical for the Court to completely overrule third-party doctrine. Overruling third-party doctrine would require voiding at least three Supreme Court cases. Although many of the Justices have expressed concern over third-party doctrine, their reasoning also shows a respect for the doctrine and a desire to make it work in the digital era.[251] For example, Chief Justice Roberts has expressed concern over third-party doctrine, but has been very clear to create exceptions and explain that his rulings are simply creating narrow carve outs, not throwing out the whole doctrine.[252]

---

248. *See supra* Sections II.B-C; c*f*. Kerr, *supra* note 155 ("So long as a person knows that they are disclosing information to a third party, their choice to do so is voluntary and the consent valid.").

249. *See supra* note 57 and accompanying text; Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 1024-26 (2007).

250. Henderson, *supra* note 249.

251. *See* Carpenter v. United States, 585 U.S. 296, 314-16 (2018) ("There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today. The Government thus is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information. . . . We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras.").

252. Riley v. California, 573 U.S. 373, 385 (2014) (saying that modern cell phones "are now such a pervasive and insistent part of daily life" that they ought to be treated differently from physical objects); *Carpenter*, 585 U.S. at 309 (saying that "cell phone location information is detailed, encyclopedic, and effortlessly compiled," and so "a third party does not by itself overcome the user's claim to Fourth Amendment protection," and "when considering new

As discussed in Section IV.D, the Justices may be skeptical of the Purpose-Sensitivity approach as well, but it holds more promise than a complete overruling of third-party doctrine. Second, as this Note has shown with the Purpose-Sensitivity approach, there is value in third-party doctrine, and there is a place for it—it simply needs to be reworked for location data.

Lastly, many scholars argue that we should fundamentally change third-party doctrine and in particular believe that the Court got it wrong in *Carpenter*. It is true that *Carpenter* left uncertainty over how, if at all, to apply third-party doctrine. However, *Carpenter* provided useful lessons and language on third-party doctrine. Scholars who want to overturn *Carpenter* often fall into two buckets. One is the "return to property" approach and the other is "return to *Katz*." The return to property approach would have courts inquire into whether the information searched is the property of the user.[253] It also advocates for examining whether a trespass occurred when law enforcement conducted a search.[254] This approach is too narrow and does not consider the changing technological landscape. In today's digital age, whether something is someone's property is very unclear,[255] and when third parties are involved it becomes even less clear. The Court has already begun to recognize the limitation of this property approach, which is why it has shifted to a privacy inquiry. Thus, a return to a property approach would require overturning precedent and contradicting the Court's reasoning that favors privacy over property. As such, a property approach is not in line

innovations . . . the Court must tread carefully in such cases, to ensure that we do not 'embarrass the future'" (quoting Nw. Airlines v. Minnesota, 322 U.S. 292, 300 (1944))).

253. *See, e.g.*, Nicholas A. Kahn-Fogel, *Property, Privacy, and Justice Gorsuch's Expansive Fourth Amendment Originalism*, 43 HARV. J.L. & PUB. POL'Y 425, 467 (2019); Donald L. Buresh, *The Meaning of Justice Gorsuch's Dissent in* Carpenter v. United States, 43 AM. J. TRIAL ADVOC. 55, 101 (2019); Laura K. Donohue, *Functional Equivalence and Residual Rights Post-Carpenter: Framing a Test Consistent with Precedent and Original Meaning*, 2018 SUP. CT. REV. 347, 400; Solove, *supra* note 57 ("The third party doctrine presents one of the most serious threats to privacy in the digital age.").

254. *Carpenter*, 585 U.S. at 383.

255. The issue of property ownership and data is largely debated in the field of intellectual property law. *See, e.g.*, Ignacio Cofone, *Beyond Data Ownership*, 43 CARDOZO L. REV. 501, 501 (2021) (explaining the "flaws of a property approach to personal information. Such an approach magnifies well-known problems of consent in privacy law: asymmetric information, asymmetric bargaining power, and leaving out inferred data. It also creates a fatal problem: moral hazard where corporations lack incentives to mitigate privacy harm.").

with Fourth Amendment jurisprudence, which has made clear that the Fourth Amendment protects people, not property.[256]

As was previously discussed, the return to *Katz* approach is most represented by Jacobi and Stonecipher, who want to examine reasonableness of privacy by looking at whether information was "knowingly exposed" and "to the public."[257] Like Kerr, they propose that courts could examine the users' consent alongside "contracts and terms of service."[258] However, determining informed choice or what a "reasonable person" should have known in the digital age has proven difficult for courts.[259] For these reasons, purpose is preferred to knowledge because it "depend[s] on the actual state of mind of the actor rather than on what a reasonable man in the circumstances would have contemplated."[260] This means that the actual actor's intent is more valuable than a hypothetical person's reasonable knowledge. This is why the Purpose-Sensitivity approach looks beyond "knowingly exposed" and instead looks at the user's purpose, and specifically, if they purposefully shared the data with the public.[261] Additionally, a knowledge inquiry and a full return to the *Katz* reasonableness test has proven challenging because what a reasonable man should know is unworkable and unjust in an age where regular people adopt new technologies on a regular basis.[262]

Lastly, the return to *Katz* argument usually disregards the arguments made in *Carpenter* and thus would require overruling *Carpenter*. Jacobi and Stonecipher argue that *Carpenter* created an exception that is unworkable and out of line with jurisprudence.[263] However, much of the logic in

256. Katz v. United States, 389 U.S. 347, 353 (1967) ("[O]nce it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion . . . .").

257. Jacobi & Stonecipher, *supra* note 44, at 873.

258. *Id*. at 877.

259. The Fifth Circuit and Fourth Circuit split on this exact issue. *See supra* Section II.B.

260. *See supra* note 180 and accompanying discussion.

261. *See supra* Section III.A for a discussion of the difference.

262. *See supra* note 181 ("It was believed to be unjust to measure liability for serious criminal offenses on the basis of what the defendant should have believed or what most people would have intended.").

263. Jacobi & Stonecipher, *supra* note 44, at 859-60.

Carpenter is in line with precedent and the intent of the Fourth Amendment.[264] Beyond this, if *Carpenter* is overruled and courts move to the two-prong test Stonecipher and Jacobi recommend, courts would only look at "knowingly exposed" and "to the public" to determine reasonableness of the expectation of privacy. This completely disregards precedent that looks at the "nature of the particular documents sought."[265] If courts looked at only these two factors, there would be no consideration of or inquiry into actual privacy, which is a well-recognized and long-held concern of the Court.[266] In contrast, the Purpose-Sensitivity approach considers the reasoning in *Carpenter* as well as *Katz* and creates a path forward that encompasses both. In this way, the approach is more implementable, because it does not require the Court to overturn or toss aside any precedent and instead unifies the Court's precedent. Importantly, the Court declined to take either the return to *Katz* or the return to property approach in *Carpenter*,[267] highlighting the impracticality of these proposals.

D. Drawbacks

Despite being consistent with jurisprudence, responsive to critiques, and feasible under the current Court, the Purpose-Sensitivity approach is not without its drawbacks. This Section responds to three in particular: (1) it does not create a simple bright-line rule; (2) it could be seen as weakening the doctrine too much; and (3) it may face challenges in implementation. None of these are insurmountable.

One possible critique of the Purpose-Sensitivity approach is that it does not create a bright-line rule, making it difficult to apply. This critique is similar to a common critique of Fourth Amendment jurisprudence, that it is unclear and challenging to implement. However, the Purpose-Sensitivity approach aims to provide more clarity and detail to guide courts. The specific factors under each prong are crucial here. The test draws directly from *Katz*, *Carpenter*, *Smith*, and *Miller*.[268] It is also informed by the reasoning in the circuit courts, which have already used the reasoning

264. *See supra* Sections II.A and IV.A.

265. Carpenter v. United States, 585 U.S. 296, 314 (2018).

266. *See, e.g.*, Riley v. California, 573 U.S. 373, 393-400 (2014); United States v. Miller, 425 U.S. 435, 440-43 (1976); Smith v. Maryland, 442 U.S. 735, 739-45 (1979).

267. *Carpenter*, 585 U.S. at 306, 313-18.

268. *See supra* Section IV.A.

embedded in the test.[269] Fourth Amendment questions will almost never be clear-cut, but the Purpose-Sensitivity approach provides a more workable solution than current third-party doctrine and many other proposed inquiries. Third-party doctrine has a clear-cut rule but a difficult test, whereas the Purpose-Sensitivity approach is not a bright-line rule but a flexible and fact-dependent test that is easy to apply.

Another possible critique is that the proposed test weakens third-party doctrine too much, disrupting the balance between privacy and crime prevention. This argument would likely come from scholars who agree with Orin Kerr's arguments about the third-party doctrine being a necessary and useful tool.[270] However, as this Note has shown, there are real concerns with how expansive third-party doctrine has become and how it has whittled away at Fourth Amendment protections. Additionally, although the Purpose-Sensitivity approach may seem less stringent on users than prior applications of third-party doctrine, it is in line with precedent and the Fourth Amendment. As such, it is an appropriate way to adapt third-party doctrine for location data.

A third critique is that this test may not be popular with the current Court, given that there is a conservative majority. One reason for this is that some of the conservative Justices have shown a strong inclination for returning to a property-based approach. However, in *Carpenter*, the majority of the Court chose not to apply a property approach to technology and data.[271] Still, Justice Gorsuch[272] and Justice Thomas[273] have indicated a preference for a return to a property-based approach. While true, Justice Gorsuch bases much of his critiques on the pitfalls of the *Katz* test and on the difficulty in applying this standard.[274] The new test responds to these

269. *See supra* Sections II.B and III.C.

270. *See supra* Section IV.C.2.

271. Carpenter v. United States, 585 U.S. 296, 322 (2018) (Kennedy, J., dissenting) ("In concluding that the Government engaged in a search, the Court unhinges Fourth Amendment doctrine from the property-based concepts that have long grounded the analytic framework that pertains in these cases.").

272. *Id.* at 357 (Gorsuch, J., dissenting) ("That the *Katz* test departs so far from the text of the Fourth Amendment is reason enough to reject it.").

273. *Id.* at 342 (Thomas, J., dissenting) ("This case should not turn on 'whether' a search occurred. It should turn, instead, on whose property was searched." (citation omitted)).

274. *Id.* at 395 (Gorsuch, J., dissenting) ("Resorting to *Katz* in data privacy cases threatens more of the same. . . . While surely laudable, these principles don't offer lower courts much guidance.")

concerns with *Katz* by combining it with *Carpenter* and bringing it in line with *Smith* and *Miller*. Justice Thomas on the other hand argues that the *Katz* test strays too far from the text and intent of the Fourth Amendment.[275] The proposed new test, however, brings *Katz* and third-party doctrine closer to the intent of the Fourth Amendment. As such, this new test will likely appeal to Justice Thomas and Justice Gorsuch as compared to alternatives.

Other members of the Court's conservative majority are opposed to a property-based approach.[276] For example, Justice Alito in *Jones* criticized the majority for applying a trespass approach to modern technology.[277] Justice Alito also seemed inclined to find a more coherent way to apply third-party doctrine in *Carpenter*.[278] Chief Justice Roberts has also signaled that he does not favor a property-based approach and thinks the Court needs a new test for technology.[279] The Purpose-Sensitivity approach could be attractive to these Justices, because it provides clarity and a straightforward test for applying third-party doctrine to location data. The Court is unlikely to favor a property-based approach, given its general hesitancy to apply another unworkable test that would create more challenging applications to data.[280]

The Purpose-Sensitivity approach shows actual promise for convincing originalists like Justice Alito and Justice Roberts. As for the newer conservative Justices, Justice Kavanaugh and Justice Barrett, it has yet to be

275. *Id.* at 343 (Thomas, J., dissenting).

276. United States v. Jones, 565 U.S. 400, 414 (2012) (Sotomayor, J., concurring) ("[T]he trespassory test applied in the majority's opinion reflects an irreducible constitutional minimum" but "even in the absence of a trespass, 'a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.'" (quoting Kyllo v. United States, 533 U.S. 27, 33 (2001))).

277. *Jones*, 565 U.S. at 420 (Alito, J., concurring).

278. *Carpenter*, 585 U.S. at 346 (Alito, J., dissenting) ("Although the majority professes a desire not to 'embarrass the future,'" that may mean that instead "this Court will face the embarrassment of explaining in case after case that the principles on which today's decision rests are subject to all sorts of qualifications and limitations that have not yet been discovered. . . . [W]e will inevitably end up 'mak[ing] a crazy quilt of the Fourth Amendment.'" (citations omitted)).

279. Riley v. California, 573 U.S. 373, 385 (arguing that because cell phones "are now such a pervasive and insistent part of daily life," they ought to be treated differently from physical objects.).

280. *See* Jacobi & Stonecipher, *supra* note 44, at 865-66.

seen how they would apply third-party doctrine. But they may be convinced by the Purpose-Sensitivity approach for the same reasons Justice Gorsuch, Justice Thomas, Justice Roberts, and Justice Alito might be, and because it is informed by the conservative Fifth Circuit's decision.

One last critique of the proposed test is two-part. First, critics might ask if courts should even be guiding Fourth Amendment protections, or if the legislature would be a more appropriate option. They might then ask if courts have the institutional capacity to undertake this test. The first concern is popular among scholars who believe courts are stripping Fourth Amendment protections[281] and has been suggested by Justice Gorsuch as well.[282] After *Smith* and *Miller*, the legislature was the go-to institution for attempting to create Fourth Amendment protections. However, a legislative solution is not desirable for location-data-related Fourth Amendment problems. The situations and contexts discussed here are so particular that broad-based protections from the legislature are inappropriate. A granular fact-based approach is necessary to ensure that any Fourth Amendment test related to location data is in line with the original intent of the Amendment while still safeguarding rights. Lastly, those who propose legislation often do so because they think the courts are weakening the Fourth Amendment, but it is unclear whether Congress would strengthen the Fourth Amendment. Conversely, the proposed Purpose-Sensitivity approach strengthens Fourth Amendment protections.

The second concern centers on the capacity of courts to undertake this approach. This concern is often brought up by scholars like Orin Kerr who favor maintaining the third-party doctrine.[283] This is in part because they believe third-party doctrine provides an easy bright-line rule for courts to apply, thereby not wasting the judiciary's resources with complex inquiries. However, this is not true. Third-party doctrine is not easily applied to location data and courts expend significant resources trying to determine whether to apply the doctrine. The circuit split perfectly shows how third-party doctrine is unmanageable, as the specific question of third-party doctrine was appealed and the Fourth Circuit even granted rehearing en banc. Of course, the Purpose-Sensitivity approach will also be complicated,

281. Noah Chauvin, *New Legislation Would Close a Fourth Amendment Loophole*, BRENNAN CTR. FOR JUST. (July 6, 2023), https://www.brennancenter.org/our-work/analysis-opinion/new-legislation-would-close-fourth-amendment-loophole/ [https://perma.cc/U6NP-EE4G].

282. *Carpenter*, 585 U.S. at 392 (Gorsuch, J., dissenting).

283. *See supra* note 236.

but it allows courts to use familiar tools and existing case law to answer the third-party question.

For example, courts have case law for both aspects of the test. For the Purpose prong, they can rely on Fourth Amendment jurisprudence that looked at whether something was public or private.[284] Further, because the test proposes looking at purpose, much like the criminal legal system does with mens rea, it is already clear that courts can make this inquiry. Indeed, all circuits have had to examine purpose for mens rea, as has the Supreme Court.[285] For the Sensitivity prong, courts also have an expanse of Fourth Amendment precedent unrelated to third-party doctrine to rely on.[286] They also have case law related to technology and sensitivity, as well as Supreme Court reasoning that can guide them. Because third-party doctrine already stretches the institutional capacity of the judiciary, and the proposed test is guided by jurisprudence and other legal inquiries, the argument that courts do not have the capacity for this test is unconvincing.

V. CONCLUSION

Today, we use our phones to do everything, and we especially use them for location services. Most people could not find their way around without their phone, let alone explore a new place. And even non-location-based phone apps track and store our location data. With the current state of third-party doctrine, all of this is fair game for the government to search. Given the vast amount of sensitive location data we share with third parties, this is concerning and shows just how ill-suited third-party doctrine is for

284. *See supra* Section III.A.

285. *See, e.g.*, United States v. George, 386 F.3d 383 (2d Cir. 2004); United States v. Smith, 104 F.4th 314 (D.C. Cir. 2024); United States v. Brasby, 61 F.4th 127 (3d Cir. 2023); United States v. Bailey, 444 U.S. 394, 404 (1980) (noting that "a person who causes a particular result is said to act purposefully if 'he consciously desires that result, whatever the likelihood of that result happening from his conduct'" (quoting United States v. U.S. Gypsum Co., 438 U.S. 422, 445 (1978))); United States v. Qureshi, 121 F.4th 1095 (5th Cir. Nov. 20, 2024); United States v. Kinard, 93 F.4th 213 (4th Cir. 2024); Bennett v. United States, 868 F.3d 1, *withdrawn and vacated*, 870 F.3d 34 (1st Cir. 2017); United States v. Carr, 107 F.4th 636 (7th Cir. 2024); United States v. Skouteris, 51 F.4th 658 (6th Cir. 2022); United States v. Lyman, 991 F.3d 994 (8th Cir. 2021); United States v. Duldulao, 87 F.4th 1239 (11th Cir. 2023); United States v. Gomez, 115 F.4th 987 (9th Cir. 2024); United States v. Hernandez-Hernandez, 519 F.3d 1236 (10th Cir. 2008).

286. *See supra* Section III.B.

location data in our digital age. In response, this Note's test centers on whether the user purposefully shared their location data with the broad public and if the location data contains or could contain sensitive information. This Purpose-Sensitivity approach is grounded in jurisprudence, responsive to concerns, workable for the courts, and rooted in the intent of the Fourth Amendment. And the good news is, with the Purpose-Sensitivity approach, you can use Find My Friends *and* keep your privacy.