Texas Law Review Online

Volume 99

Note

The Mosaic Theory's Two Steps: Surveying *Carpenter* in the Lower Courts

Taylor H. Wilson, Jr.[†]

Abstract

In Carpenter v. United States*, the Supreme Court announced that seven days' worth of historical cell-site location information (CSLI) was a "search" within the meaning of the Fourth Amendment. Scholars and lawyers have argued that this holding reflected the "mosaic theory" of the Fourth Amendment—considering a series of governmental actions in aggregate when evaluating whether a search occurred. But this argument does not capture the full picture. This Note posits that the Supreme Court's decision in* Carpenter *reflected a new approach to the mosaic theory. A close reading of* Carpenter*, when compared to* United States v. Jones*, shows that the Court focused on the nature of information that CSLI conveys prior to considering the amount gathered in the case.* Carpenter*'s new mosaic theory has two steps—whether the data, when aggregated, has the potential to violate a reasonable expectation of privacy, then whether the information obtained in the present case did so.*

*This Note surveys post-*Carpenter *decisions in federal and state courts, finding that* Carpenter*'s focus on the nature of information obtained has been adopted by many lower courts. Through this analysis, this Note concludes that* Carpenter*'s two-step mosaic theory is an improvement on* Jones*'s one-*

[†] J.D. Candidate, Class of 2021, The University of Texas School of Law. Special thanks to Grace Carpenter and Sarah Propst for their feedback and support. I owe a debt of gratitude to *Texas Law Review Online* editors for their careful edits and helpful comments. Any mistakes are mine alone.

step approach. The two-step approach allows lower courts to draw bright lines based on the type of data involved. Additionally, the two-step mosaic theory provides a doctrinal means to base Fourth Amendment search inquiries on the nature of the information acquired, rather than the amount obtained.

Introduction

The Supreme Court's decision in *Carpenter v. United States*[1] heralded a new age of Fourth Amendment doctrine. Professor Orin Kerr, for instance, termed it a "blockbuster" decision.[2] Professor Rachel Levinson-Waldman called it a "landmark privacy case."[3] Professor Paul Ohm argued that it is "likely to guide the evolution of constitutional privacy in this country for a generation or more."[4] And *Carpenter* indeed opened up a new avenue for Fourth Amendment analysis of digital data. Prior to *Carpenter*, the Court had adopted a sequential approach to assessing digital data. Courts considered government actions individually when evaluating whether conduct was a "search" within the meaning of the Fourth Amendment. But the majority in *Carpenter* rejected that approach. Seven days' worth of records of historical cell-site location information (CSLI), when considered in aggregate, qualified as a search because it violated a person's "legitimate expectation of privacy in the record of his physical movements."[5]

Carpenter's shift has led to confusion about the place of the "mosaic theory" in Fourth Amendment doctrine. As Professor Kerr defines the concept, the mosaic theory asks "whether a series of acts that are not searches in isolation amount to a search when considered *as a group*."[6] In *Carpenter*, the Court seemed to accept the mosaic theory by considering the data presented as a group.[7] But, at the same time, the Court appeared to reject the mosaic theory: "[W]e need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be."[8]

---

1. 138 S. Ct. 2206 (2018).

2. Orin S. Kerr, *Implementing* Carpenter, *in* THE DIGITAL FOURTH AMENDMENT 1 (forthcoming), https://ssrn.com/abstract=3301257.

3. Rachel Levinson-Waldman, *Supreme Court Strengthens Digital Privacy*, BRENNAN CENTER (June 22, 2018), https://www.brennancenter.org/our-work/analysis-opinion/supreme-court-strengthens-digital-privacy [https://perma.cc/T7NT-9J4V].

4. Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 358 (2019).

5. *Carpenter*, 138 S. Ct. at 2217.

6. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 320 (2012) (emphasis added).

7. *See Carpenter*, 138 S. Ct. at 2217 (discussing how cell-phone location data "over the course of 127 days" can provide an "all-encompassing record" of the user's location).

8. *Carpenter*, 138 S. Ct. at 2217 n.3.

This Note argues that *Carpenter* did invoke the mosaic theory in its reasoning but added a step to the process. Pre-*Carpenter* decisions considered the mosaic theory as part of a single multifactor test: Did the information in the present case, when aggregated, violate a reasonable expectation of privacy? The concurrences in *Jones* reflected this approach, setting the inquiry against the facts of the case—28 days of GPS tracking data. The new mosaic theory has two steps: (1) Does the information obtained, when aggregated, have the potential to violate a reasonable expectation of privacy? (2) Did the information in the present case do so? This reading stems from the majority decision in *Carpenter*, which considered the potential of what historical CSLI *could* reveal prior to applying the facts of the case.

This distinction may assist lower courts in applying *Carpenter*. A survey of lower court decisions reveals a wide array of challenges to digital surveillance in the post-*Carpenter* era.[9] Courts have adopted varying approaches—some use the *Jones* model of a single multifactor test,[10] but others have echoed *Carpenter* and elevated the nature of information obtained to be a dispositive factor.[11] This Note argues that the latter approach is preferable. Prioritizing the nature of information obtained allows courts to draw meaningful lines around the Fourth Amendment's search requirement, rather than creating arbitrary lines based on the duration of the surveillance in any individual case. Drawing these bright lines would aid both citizens (by allowing the threshold for a search to modulate as technology changes) and law enforcement (by giving notice as to when search warrants are necessary).

This Note begins, in Part I, by examining the mosaic theory's place in Fourth Amendment doctrine and the "reasonable expectation of privacy" test from *Katz v. United States*.[12] It continues to define the mosaic theory, discuss criticisms of the mosaic theory, and distinguish between the one-step and two-step approaches. Part II surveys lower court decisions since *Carpenter* in light of the two mosaic theories. It groups cases by the type of data obtained and suggests that many courts consider aggregated data's potential to violate a reasonable expectation of privacy when conducting a *Katz* analysis. This Note concludes by discussing the implications of the two-step mosaic theory. It posits that the two-step approach produces a more effective common law system by requiring lower courts to discuss why they believe a type of data should or should not be private. Finally, it argues that the two-step mosaic theory could serve as a transition to a broader standard based on the type of information obtained by police.

---

9. *See* Part III, *infra*.

10. *See* subpart II(B), *infra*.

11. *See* subpart II(B), *infra*; *see, e.g.*, State v. Sylvestre, 254 So.3d 986, 991 (Fla. Ct. App. 2018).

12. 389 U.S. 347 (1967).

I. The Fourth Amendment and the Mosaic Theory

A. The Reasonable Expectation of Privacy Test

For the Fourth Amendment to apply, a government action must be a "search" or "seizure."[13] Though the doctrine originally focused on physical intrusion into protected spaces, it evolved into a test based on a person's "reasonable expectation of privacy." Justice Harlan provides the best explanation of this test in his concurrence in *Katz v. United States*: If a person has a subjective expectation of privacy that society is prepared to recognize as reasonable, then an action violating that expectation is a search.[14] Some later cases have shortened this test—if government action violates a person's reasonable expectation of privacy, it is a search.[15]

The key dispute in the expectation-of-privacy test is what makes an expectation "reasonable."[16] The Supreme Court has never explained which factors should be considered.[17] In some cases, it asks if it is likely that a person or place would be observed or investigated.[18] In another line of cases, the Court asks if the nature of the information obtained is particularly private or personal.[19] In a third set, the Court asks if another source of law prohibited the government's conduct.[20] And in a fourth set, the Court weighs normative

13. The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

14. *Katz*, 389 U.S. at 361.

15. *See, e.g.*, Oliver v. United States, 466 U.S. 170, 178 (1984); Terry v. Ohio, 392 U.S. 1, 9 (1968) ("[W]herever an individual may harbor a reasonable 'expectation of privacy,' he is entitled to be free from unreasonable government intrusion."). *Cf.* Orin S. Kerr, Katz *Has Only One Step*, 82 U. CHI. L. REV. 113, 114 (finding that lower courts generally adhere to this one-step test).

16. Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 504 (2007).

17. *See, e.g.*, *Oliver*, 466 U.S. at 177 ("No single factor determines whether an individual legitimately may claim under the Fourth Amendment that a place should be free of government intrusion not authorized by warrant."). *See also* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.1(a) (5th ed. 2019).

18. *See, e.g.*, Bond v. United States, 529 U.S. 334, 338–39 (2000) (reasoning that a bus passenger "does not expect that other passengers or bus employees will, as a matter of course, feel the bag in an exploratory manner"). Professor Kerr terms this standard the "probabilistic" model. Kerr, *supra* note 16, at 508.

19. *See, e.g.*, Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986) ("[T]he photographs here are not so revealing of intimate details as to raise constitutional concerns."). Kerr terms this the "private facts" model. Kerr, *supra* note 16, at 512.

20. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 451 (1989) (plurality opinion) (holding that surveillance by helicopter was not a search but noting that the Court "would have a different case if flying at that altitude had been contrary to law or regulation"). Kerr terms this view the "positive law" model. Kerr, *supra* note 16, at 516.

arguments and bases its holding on policy grounds.[21] But the Court often modulates between these rationales, and lower courts have operated similarly.[22]

B. The Mosaic Theory

Because expectations of privacy can change over time, courts have struggled with applying the *Katz* standard in novel contexts—especially with respect to digital data. After all, public and private actors can now monitor us "in ways that once seemed like science fiction."[23] Traditionally, courts used a sequential approach to analyze Fourth Amendment issues.[24] Whether a search occurred depends on a "frame-by-frame dissection" of the facts.[25] If an action in any of those frames violated a reasonable expectation of privacy, a search occurred at the moment that the action exposed information.[26] If police opened a door to enter an apartment, moved a couch, and flipped the couch over, each of those three actions would have to be analyzed under the *Katz* standard.

Government access to digital data challenged the sequential approach. The sequential approach works when discrete steps are involved—opening a door, moving a stereo, entering a backyard. But digital data is made up of small bits of information, which on their own may not convey significant information. Enter the mosaic theory. The mosaic theory suggests that "a series of acts that are *not* searches in isolation amount to a search when considered *as a group*."[27] One court has termed it an aggregation principle for technological surveillance.[28] As the analogy goes, "the color of a single stone depicts little, but by stepping back one can see a complete mosaic."[29]

The mosaic theory originated in *United States v. Jones*,[30] a case about tracking a suspect with a GPS device for twenty-eight days.[31] Writing for a

21. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 34 (2001) (holding that use of a thermal imaging device on a home was a search because the holding would "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted"). Kerr calls this view the "policy model." Kerr, *supra* note 16, at 519.

22. *See* Kerr, *supra* note 16, at 526 (arguing that this modulation allows lower courts to develop rules that draw clear lines for police to follow).

23. David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N. CAR. J.L. & TECH. 381, 386 (2013).

24. Kerr, *supra* note 6, at 315.

25. *Id.* at 316.

26. *Id.* at 317.

27. Kerr, *supra* note 6, at 320 (emphasis added); Gray & Citron, *supra* note 23, at 397 ("[W]e can maintain reasonable expectations of privacy in certain quantities of information and data even if we lack reasonable expectations of privacy in the constituent parts of those wholes.").

28. Commonwealth v. McCarthy, 142 N.E.3d 1090, 1102 (Mass. 2020).

29. *Id.*

30. 565 U.S. 400.

31. *Id.* at 403.

four-Justice concurrence, Justice Alito incorporated the amount of data as a factor in the *Katz* standard. He drew a line between short-term and long-term monitoring of someone driving in public.[32] Society would not expect that police would "secretly monitor and catalogue every single movement" of a car for "a very long period."[33] Similarly, Justice Sotomayor argued the Court should consider whether an expectation of privacy existed "in the sum of one's public movements."[34] Both of these concurrences argued for considering the GPS data in aggregate when applying the *Katz* test.

The Supreme Court applied the mosaic theory to a different kind of data in *Carpenter v. United States*.[35] *Carpenter* concerned historical cell-site location information (CSLI)—data indicating that a cell phone connected to a certain cell tower at a certain time.[36] Police had acquired 12,898 location points cataloguing the defendant's movements.[37] The Supreme Court held that this action was a search.[38] It focused on the nature of the information obtained—"the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection."[39] Similarly, it rejected the argument that the third-party doctrine applied to the case.[40] The court reasoned that *Smith* and *Miller* required examining the "nature of the particular documents" law enforcement accessed.[41] Because CSLI revealed location information, and revealed it involuntarily, the Court held that the third-party doctrine should not apply.[42] However, the Court cabined its holding to historical CSLI, refusing to evaluate real-time CSLI, "tower dumps,"[43] or "conventional surveillance techniques and tools," like security cameras.[44] Moreover, the Court declined to answer if acquiring a limited period of historical CSLI would be a search.[45] For the Court, seven days of CSLI was sufficient to violate a reasonable expectation of privacy.

---

32. *Id.* at 430 (Alito, J., concurring in the judgment).

33. *Id.*

34. *Id.* at 416 (Sotomayor, J., concurring).

35. 138 S. Ct. 2206 (2018).

36. *See id.* at 2211–12 (describing historical CSLI).

37. *Id.* at 2212.

38. *Id.* at 2217.

39. *Id.* at 2223.

40. The third-party doctrine posits that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Smith v. Maryland, 442 U.S. 735, 743–44 (1979); *see also* United States v. Miller, 425 U.S. 435, 442–44 (1976) (same).

41. *Carpenter*, 138 S. Ct. at 2219.

42. *Id.* at 2219–20.

43. A tower dump is a download of all the CSLI data for all users that accessed a single cell phone tower over an interval of time. *See* section III(A)(3), *infra*.

44. *Carpenter*, 138 S.Ct. at 2220.

45. *Id.* at 2217 n.3.

C. Criticisms and Responses to the Mosaic Theory

The mosaic theory has faced criticism by both courts and scholars.[46] The most prominent criticisms key in on practical concerns: (1) the scope of the theory's aggregation principle and (2) the theory's requirement of case-by-case analysis. First, underlying the mosaic theory is an aggregation principle—data should be considered as an aggregated whole rather than piecemeal.[47] But this premise requires courts to draw lines it may not be equipped to do.[48] Should a court aggregate only one's individual data? What if the surveillance gathers other peoples' data as well?[49] Should a court aggregate data even if it is not continuous?[50] Or even if the data is spread across multiple types of surveillance?[51] Most importantly, what is the amount of data that violates a reasonable expectation of privacy?[52] As one court put it, drawing these lines is "arbitrary and unrelated to a reasonable expectation of privacy."[53]

Second, the mosaic theory would require case-by-case analysis—did the amount of data *in the present case* violate a reasonable expectation of privacy?[54] The sequential approach is categorical—conduct is either always or never a search.[55] Conversely, the mosaic theory requires courts to evaluate each case individually. This requirement puts law enforcement in a bind. Say that an officer wants to query a database. Under the mosaic theory, officers

---

46. *See, e.g.*, United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010) (Sentelle, J., dissenting) (arguing that "[t]he sum of an infinite number of zero-value parts is also zero"); Kerr, *supra* note 6, at 329–30 (listing major objections to the theory).

47. *See* Kerr, *supra* note 6, at 320 (noting that the theory is "premised on aggregation").

48. *See, e.g.*, *McCarthy*, 142 N.E.3d at 1106 ("[W]e cannot say precisely how detailed a picture of the defendant's movements must be to invoke constitutional protections . . . ."); Commonwealth v. Mora, 150 N.E.3d 297, 312 Mass. 2020) ("We need not decide in this case where [the] boundary lies.").

49. *See* subpart III(B), *infra* (discussing cell-site simulators).

50. *See* Leaders of a Beautiful Struggle v. Balt. Pol. Dep't, 456 F.Supp.3d 699 (D.Md. 2020) (refusing to aggregate video data from aerial surveillance because the planes "will not fly at night").

51. *See* Kerr, *supra* note 6, at 335–36 (explaining this concern).

52. *See* United States v. Jones, 565 U.S. 400 (2012) (criticizing Justice Alito for failing to define "why a 4-week investigation is 'surely' too long").

53. State v. Muhammad, 451 P.3d 1060, 1073 (Wash. 2019). *See* Kerr, *supra* note 6, at 344 (calling this line-drawing an "awkward halfway measure"). *But see* Gray & Citron, *supra* note 23, at 424 ("It is hard to see how the line-drawing concerns raised by mosaic critics are any more worrisome than the line-drawing problems that are inherent to the Fourth Amendment.").

54. *See* United States v. Maynard, 615 F.3d 544, 563 (D.C. Cir. 2010) (holding that twenty-eight days of GPS surveillance was a search), *aff'd sub nom. Jones*, 565 U.S. at 404. *But see Carpenter*, 138 S. Ct. at 2217 n.3 (declining to answer if accessing fewer than seven days' worth of historical CSLI data would be a search).

55. Kerr, *supra* note 6, at 344. *See Katz*, 389 U.S. at 35 (holding that tapping a phone booth is always a search); United States v. Karo, 468 U.S. 705, 718 (drawing a bright line between GPS surveillance in public locations and in private locations).

can only know if they needed a warrant until after they already conducted a warrantless search.[56] It requires officers to make uninformed *ex ante* judgments about how a court will view the facts *ex post*.

Scholars have proposed alternatives to the mosaic theory that remedy these problems. Professors Gray and Citron argue that courts should focus on "*how* information is gathered," not "*how much* information is gathered in a particular case."[57] In their view, the threshold question should be whether an investigative technology "has the capacity to facilitate broad programs of indiscriminate surveillance" that could "raise the specter of a surveillance state" if left to the government.[58] Factors would include: (1) the technology's surveillance capabilities, (2) the technology's scale, and (3) the costs of deploying and using the technology.[59] This standard would be categorical—if the technology had the capability to indiscriminately surveil, then using it would be a search.[60]

Professor Kerr makes a similar proposal, which he terms the "Source Rule."[61] Whether accessing information is a search should be dependent on the "use of a technology that *Carpenter* covers."[62] If law enforcement "learned any fact sourced from any *Carpenter*-covered record, then that information transfer is a search."[63] Three factors would make data protected under *Carpenter*: (1) it could not be collected in a pre-digital age, (2) it is created without one's "meaningful voluntary choice," and (3) it tends to reveal "an intimate portrait of a person's life."[64] This standard would also be categorical—if the data is protected under *Carpenter*, then revealing the data would be a search.[65]

D. How Carpenter Changed the Mosaic Theory

In *Carpenter*, the Court adopted a standard that incorporates these criticisms while adhering to past precedent. The term "mosaic theory" refers to two different standards—a one-step and two-step version of the same concept. The one-step mosaic theory reflects the approaches of Justices Alito and

56. Orin S. Kerr, *Automated License Plate Readers, the Mosaic Theory, and the Fourth Amendment*, VOLOKH CONSPIRACY (Apr. 22, 2020), https://reason.com/2020/04/22/automated-license-plate-readers-the-mosaic-theory-and-the-fourth-amendment/ [https://perma.cc/9KDF-2BMN].

57. David Gray & Danielle Keats Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 71 (2013).

58. *Id.* at 101.

59. *Id.* at 102.

60. *See id.* (positing that litigants could challenge this conduct once the surveillance technology is "identified as implicating the Fourth Amendment").

61. Kerr, *supra* note 2, at 28.

62. *Id.*

63. *Id.*

64. *Id.* at 16, 20, 22.

65. *See id.* at 40 ("One datum is just as protected as the entire database. It's all protected.").

Sotomayor in *Jones*. Whether a government action is a search depends on the nature of information obtained *in the present case*, which includes amount as a factor.[66] A court should consider multiple factors in its analysis and evaluate new technologies on the facts of the case before it.[67]

Carpenter reflects a different version of the mosaic theory—one in which the type of information obtained is a dispositive factor. The new mosaic theory has two steps: (1) Does the data, in aggregate, have the potential to violate a reasonable expectation of privacy by revealing the "privacies of life?"[68] (2) Did the amount of data obtained in the present case do so?

This two-step mosaic theory stems from a close reading of *Carpenter*. The majority reasoned that acquiring historical CSLI *could* violate a reasonable expectation of privacy because of the information it provides:

> As with GPS information, the time-stamped data provides 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." . . . . These location records "hold for many Americans the 'privacies of life.'"[69]

This language accords with the Supreme Court's focus—from *Riley* and *Jones*—on limiting government access to data revealing "associational freedoms and intimate facts."[70] But Chief Justice Roberts considered the information that historical CSLI could reveal when aggregated. "Mapping a cell phone's location *over the course of 127 days*" reveals an "all-encompassing record" of one's locations.[71] It is this data—collectively—that provides an "intimate window" into one's life.[72]

---

66. *See Jones*, 565 U.S. at 430 (Alito, J., concurring in the judgment) ("The best that we can do in this case is . . . to ask whether the use of GPS tracking *in a particular case* involved a degree of intrusion that a reasonable person would not have anticipated.") (emphasis added).

67. *See* Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J. L. & TECH. 357, 361 (2019) (reading *Carpenter* as promoting a single-step multifactor test based on "the deeply revealing nature" of the information, its "depth, breadth, and comprehensive reach," and "the inescapable and automatic nature of its collection"); Matthew Tokson, *The Emerging Principles of Fourth Amendment Privacy*, 88 GEO. WASH. L. REV. 1, 13 (2020) (arguing that there are "three emerging principles of privacy" that shape the *Katz* inquiry, including "the intimacy of the place or thing targeted," the "amount of information sought," and "the cost of the investigation," but all on a case-by-case basis).

68. *See Carpenter*, 138 S. Ct. at 2217 (noting that location records "hold for many Americans the 'privacies of life'"); Kerr, *supra* note 2, at 22 (reading *Carpenter* for this proposition).

69. *Carpenter*, 138 S. Ct. at 2217 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)) (quoting *Riley*, 134 S. Ct. 2473, 2494–95 (2014)).

70. Kerr, *supra* note 2, at 24.

71. *Carpenter*, 138 S. Ct. at 2217.

72. *Id.*

The Supreme Court considered the facts of the case only after determining that accessing historical CSLI could violate a reasonable expectation of privacy. It asserted that it "need not decide whether there is a limited period for which" acquiring historical CSLI would not be a search, nor "how long that period might be."[73] The Court established that accessing historical CSLI could be a search—all that remained was to apply the facts of the present case. This approach errs on the side of dispute resolution rather than law declaration; but, then again, most of Fourth Amendment doctrine does so as well.[74]

Carpenter essentially added a step to the Supreme Court's use of the "private facts" model. Several Supreme Court cases have focused on the "information the government collects," and consider whether the nature of that information is so private to be "worthy of constitutional protection."[75] Professor Kerr terms this approach the private facts model.[76] For example, in *Dow Chemical Co. v. United States*,[77] taking photographs of a chemical plant was not a search because it was "not so revealing of intimate details as to raise constitutional concerns."[78] Or consider *United States v. Karo*, which held monitoring a GPS beeper was a search because it revealed information about the interior of a private home.[79] *Carpenter* indicated that courts should consider the character of information that data could convey in aggregate.[80] And it added the second step to the inquiry—that courts should consider the amount of information only after considering that information's nature.

Lower courts rarely distinguish the one- and two-step mosaic theories, but many continue to apply the theory itself. Some courts retain the old mosaic theory's one-step procedure—considering the nature of the information through the facts before the court. But many courts have adopted the new mosaic theory's two-step inquiry—considering the nature of the information, in aggregate, then applying the facts of the case. This Note now turns to analysis of these decisions.

---

73. *Id.* at 2217 n.3.

74. *See* RICHARD H. FALLON, JR. ET AL., HART & WECHSLER'S THE FEDERAL COURTS AND THE FEDERAL SYSTEM 73–75 (7th ed. 2015) (describing the dispute-resolution and law-declaration models of federal courts).

75. Kerr, *supra* note 16, at 512.

76. *Id.*

77. 476 U.S. 227 (1986).

78. *Id.* at 228.

79. *Karo*, 468 U.S. at 715.

80. *See Carpenter*, 138 S. Ct. at 2217 (considering the information that historical CSLI records provide when aggregated).

II. The Mosaic Theory in the Lower Courts

Distinguishing between the one-step and two-step mosaic theories is important because they lead lower courts to focus on different forms of reasoning. *Katz* provided a multifactor standard; but by considering the amount of information gathered as part of this standard, courts miss *Carpenter*'s focus on the nature of information conveyed. Further, distinguishing these two theories would help courts determine how to apply *Carpenter*. As of March 26, 2021, only fifteen Fourth Amendment cases since *Carpenter* have used the word "mosaic."[81] And confusion continues regarding what the term "mosaic theory" actually means.[82]

This Part synthesizes *Carpenter*'s reasoning with lower court cases that have applied it over the past two years. It surveys the types of surveillance that litigants have challenged under *Carpenter*: (1) cell-site location information (CSLI), (2) cell-site simulator data, (3) GPS location data, (4) automated license plate reader (ALPR) databases, (5) pole cameras and long-term video surveillance, and (6) internet protocol (IP) address data. This Part explains the salient factors for each type of surveillance and predicts how a court applying the new mosaic theory would treat each type. And overall, this Part shows that courts have shifted from *Jones*'s one-step mosaic theory toward *Carpenter*'s two-step approach.

A. CSLI—Historical, Real-Time, and "Tower Dumps"

1. Historical CSLI

Whenever a cell phone connects to a cell tower, it creates a time-stamped record known as cell-site location information (CSLI).[83] Historical CSLI refers to large amounts of CSLI records kept in databases. Officers can

81. Per Westlaw, these cases are: United States v. Moalin, 973 F.3d 977, 991 (9th Cir. 2020); United States v. Howard, 426 F. Supp. 3d 1247, 1254 (M.D. Ala. 2019); United States v. Kubasiak, No. 18-cr-120-pp, 2018 WL 4846761, at *2 (E.D. Wis. Oct. 5, 2018); United States v. Kubasiak, No. 18-CR-120, 2018 WL 6164346, at *2 (E.D. Wis. Aug. 23, 2018); People v. Tafoya, No. 17CA1243, 2019 WL 6333762, at *8 (Colo. App. Nov. 27, 2019); Bailey v. State, No. 1D18-4514, 2020 WL 6706904, at *5 (Fla. 1st DCA Nov. 16, 2020); Commonwealth v. Comenzo, 2021 WL 616548, at *8 (Mass. Super. Ct. Jan. 11, 2021); Commonwealth v. Cruz-Gonzalez, Nos. 1977CR00467, 2020 WL 7055431, at *13 n.24 (Mass. Super. Ct. Nov. 30, 2020); Commonwealth v. Gosselin, 158 N.E.3d 8, 15–16 (Mass. 2020); *Mora*, 150 N.E.3d at 305; *McCarthy*, 142 N.E.3d at 1101; Commonwealth v. Johnson, 119 N.E.3d 669, 686 (Mass. 2019); Sims v. State, 569 S.W.3d 634, 644 (Tex. Crim. App. 2019); *Muhammad*, 451 P.3d at 1072.

82. *See, e.g.*, Matthew Tokson, *The "Mosaic Theory" and the Aftermath of* Carpenter, DORF ON LAW (Aug. 3, 2020), www.dorfonlaw.org/2020/08/the-mosaic-theory-and-aftermath-of.html (noting that "mosaic theory" is a "confusing term" and that lower courts usually "assess the amount of data or duration of surveillance" without invoking it) [https://perma.cc/7YXC-Q4WH].

83. *Carpenter*, 138 S. Ct. at 2211.

request these records for specific cell towers for a range of dates.[84] These records allow officers to connect people to certain locations at certain times. After all, people "compulsively carry cell phones with them all the time."[85]

Historical CSLI is likely a search under the two-step mosaic theory. *Carpenter* established that historical CSLI could violate a reasonable expectation of privacy. Historical CSLI can track people over long periods of time, give information about constitutionally protected places (like churches, homes, and offices), and be produced without the cell phone user realizing it. No surprise that the Court focused on these factors, then—historical CSLI's "depth, breadth, and comprehensive reach" and its "inescapable and automatic" collection.[86] Whether a search occurred would depend on the facts of the case, but seven days apparently reveals enough to reach this invasive potential.[87] Courts have generally dismissed these challenges under the good-faith exception to the exclusionary rule.[88] Some simply apply *Carpenter* when the CSLI covers more than seven days.[89]

Under the one-step mosaic theory, a court would have to consider when aggregated CSLI changes character. For example, in *People v. Edwards*,[90] the court considered the nature of aggregated CSLI with the amount of data incorporated as a factor. In its view, long-term CSLI data is "the modern day electronic equivalent of sending a government spy out to follow the defendant."[91] Short-term CSLI data "is like taking a single snapshot of that person on the street."[92] Because two days of data fit in the short-term CSLI bucket, acquiring the data was not a search.[93] Conversely, *People v. Simpson*[94] accepted *Carpenter*'s holding that historical CSLI could violate a reasonable expectation of privacy.[95] Since the difference between three days and seven days of CSLI was *de minimis*, acquiring three days' worth was a search requiring a warrant.[96] The *Edwards* court drew a line at how much data to

84. *See, e.g.*, *id.* at 2212 (noting the government requested 127 days of CSLI from MetroPCS).

85. *Id.* at 2218.

86. *Id.* at 2223.

87. *Id.* at 2217 n.3.

88. *See, e.g.*, United States v. Wilson, 960 F.3d 136, 146 (3d Cir. 2020) (dismissing claim because historical CSLI gathered in 2014 is subject to the good-faith exception); United States v. Beverly, 943 F.3d 225, 230 (5th Cir. 2019) (reversing suppression of historical CSLI because the "district court should have applied various strands of the good-faith exception").

89. *See* Holder v. State, 595 S.W.3d 691, 698 n.16 (Tex. Crim. App. 2020) ("While the Supreme Court held that a person has an expectation of privacy in at least seven days of historical CSLI, we need not go that far. The issue here is about 23 days of Appellant's CSLI.").

90. People v. Edwards, 97 N.Y.S.3d 418, 421 (N.Y. App. Div. 2019).

91. *Id.*

92. *Id.* at 422.

93. *Id.*

94. 88 N.Y.S.3d 763 (N.Y. App. Div. 2018).

95. *Id.* at 767.

96. *Id.* at 771.

aggregate; but the *Simpson* court considered historical CSLI in aggregate when evaluating its nature.[97]

2. Real-Time CSLI

Real-time CSLI refers to tracking a suspect in real time by using their cell phone. One method is to triangulate the cell phone's location using the nearest cellular towers.[98] Alternatively, officers can signal a suspect's cell phone (termed a "ping"), to which the cell phone responds with its location information.[99] In *Carpenter*, the Court expressly declined to rule on real-time CSLI.[100] But real-time CSLI can track individuals into private locations, and long-term tracking could likely reveal one's "political and religious beliefs," among other private information.[101] So, under the two-step mosaic theory, it would seem likely that real-time CSLI could violate a reasonable expectation of privacy.[102]

However, lower courts have split over how to evaluate real-time CSLI. In *Sims v. State*,[103] the court did hold that aggregated real-time CSLI could violate a reasonable expectation of privacy.[104] It reasoned that real-time CSLI records "show location information" and "are generated solely at the behest of law enforcement."[105] The court then moved to the second step of the new mosaic theory. Because the case concerned "less than three hours" of real-time CSLI, the court held that the information aggregated did not meet this threshold.[106] *State v. Muhammad* contains similar analysis at the first step but rejected the second step of *Carpenter* altogether. The court first noted that real-time CSLI can "generate a comprehensive record of a person's public

97. *See also Carpenter*, 138 S. Ct. at 2223 (2018) (considering historical CSLI's "deeply revealing nature" in its holding).

98. *See* In re U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 534 F. Supp. 2d 585, 590 (W.D. Pa. 2008) (describing this process).

99. *See* United States v. Powell, 943 F. Supp. 2d 759, 767 (E.D. Mich. 2013) (explaining this process).

100. *Carpenter*, 138 S. Ct. at 2220.

101. *See Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) ("I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."). *Cf. Karo*, 468 U.S. at 715 (holding that tracking a suspect inside a private home using a GPS beeper was a search).

102. *Cf. Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) (emphasizing that real-time GPS monitoring could violate a reasonable expectation of privacy).

103. 569 S.W.3d 634 (Tex. Crim. App. 2019).

104. *Id.* at 645.

105. *Id.* at 645 n.15.

106. *Id.* at 646. *See also id.* ("Whether a person has a recognized expectation of privacy in real-time CSLI records must be decided on a case-by-case basis.").

movements" reflecting a "wealth of detail" about her personal life.[107] However, the *Muhammad* court rejected the second step of the new mosaic theory—in the court's view, case-by-case analysis would create "practical problems" because "[t]here is no rational point to draw the line" of how much data is too much.[108] Thus, the court held that accessing real-time CSLI was a search, categorically.[109]

3. Tower Dump CSLI

A "tower dump" is a one-time download of information for the devices that connected to a cell tower during a particular interval.[110] Tower dump CSLI differs from historical and real-time CSLI because a tower dump collects data for all users within the radius, not one user specifically. In one FBI investigation, for example, a series of tower dumps produced more than 150,000 registered cell phone numbers.[111] Tower dump requests are fast becoming a part of the law enforcement toolbox,[112] potentially because

107. 451 P.3d at 1072 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).

108. *Id.* at 1072–73.

109. *Id.* at 1072. *Cf.* Reed v. Commonwealth, No. 2018-CA-001574-MR, 2020 WL 594084, at *4 (Ky. Ct. App. Feb. 7, 2020) ("[B]ecause pinging a cell phone enables the police almost instantaneously to track individuals far beyond the public thoroughfare into areas where they would have a reasonable, legitimate expectation of privacy, we conclude that a warrant is required to acquire real-time CSLI."); State v. Snowden, 140 N.E.3d 1112, 1126 (Ohio Ct. App. 2019) (holding that obtaining CSLI is a search "whether it is one day, two days, three days, or seven days or more of data obtained").

The Massachusetts Supreme Judicial Court has also held that accessing real-time CSLI is always a search, but the decisions might implicate only the Massachusetts state constitution. *See* Commonwealth v. Almonor, 120 N.E.3d 1183, 1193 (Mass. 2019) (holding that real-time CSLI violates a reasonable expectation of privacy because "society reasonably expects that the police will not be able to secretly manipulate our personal cell phones for any purpose"); Commonwealth v. Fredericq, 121 N.E.3d 166, 175 (Mass. 2019) (holding that a defendant had standing to file a Fourth Amendment claim regarding real-time CSLI obtained when he was a passenger and the driver used his cell phone); *but see* Commonwealth v. Lugo, 120 N.E.3d 1212, 1224–25 (Mass. 2019) (refusing a defendant's standing to challenge the search of another person's cell phone because they were in a car together for "less than two hours").

110. *Carpenter*, 138 S. Ct. at 2220 (2018).

111. Nate Anderson, *How "cell tower dumps" caught the High Country Bandits—and why it matters*, ARSTECHNICA (Aug. 29, 2013), https://arstechnica.com/tech-policy/2013/08/how-cell-tower-dumps-caught-the-high-country-bandits-and-why-it-matters/ 1/10.

112. *See* Zack Whittaker, *T-Mobile quietly reported a sharp rise in police demands for cell tower data*, TECHCRUNCH (July 12, 2019), https://techcrunch.com/2019/07/12/t-mobile-cell-tower-government-demands/ (noting that cell tower dump requests to T-Mobile increased by 27% from 2018 to 2019) [https://perma.cc/8F2T-RWRW]. *See also* AT&T, TRANSPARENCY REPORT 4 (Feb. 2018), https://about.att.com/ecms/dam/csr/2019/library/transparency/2018-February-Report.pdf (noting a total of 1,812 total tower dump requests in 2017) [https://perma.cc/8MTZ-JVVP]; AT&T, TRANSPARENCY REPORT 4 (Feb. 2019), https://about.att.com/ecms/dam/csr/2019/library/transparency/2019-February-Report.pdf (noting a total of 2,487 total tower dump requests in 2018) [https://perma.cc/4FFL-MU3S].

Carpenter expressly declined to hold whether accessing tower dump data is a search.[113]

Tower dumps highlight the difference between *Carpenter*'s two-step mosaic inquiry and the old one-step mosaic inquiry. Individually, tower dumps might not reveal enough about one's life to violate a reasonable expectation of privacy. As the court in *United States v. Walker*[114] reasoned, tower dumps "capture [CSLI] for a particular place at a limited time."[115] And they are akin to "conventional surveillance techniques . . . which capture data from every individual" in the relevant area.[116] So, because tower dump CSLI does not implicate "the whole of [an individual's] physical movements," the court in *Walker* held that no search had occurred.[117]

Under *Carpenter*, however, the question is whether the information obtained could violate a reasonable expectation of privacy in aggregate. Tower dump CSLI, when aggregated across multiple tower dumps, could reveal an individual's location just as historical CSLI does.[118] Moreover, tower dumps can reveal information from within constitutionally protected places—like a cell tower close to a defendant's private residence.[119] To be sure, *Carpenter*'s two-step mosaic theory might produce the same result as in *Walker*, depending on how many tower dumps occurred. But the one-step mosaic theory fails to consider tower dump CSLI in aggregate. And in doing so, the one-step mosaic theory misrepresents the investigative potential of the technology.

B. Cell-Site Simulators

A cell-site simulator—sometimes called a "Stingray," "Hailstorm," or "TriggerFish"—is "a device that locates cell phones by mimicking the service provider's cell tower (or 'cell-site') and forcing cell phones to transmit 'pings' to the simulator."[120] Federal and local law enforcement use cell-site simulators indiscriminately in investigations from violent felonies to low-

113. *Carpenter*, 138 S. Ct. at 2220.

114. 2020 WL 4065980 (E.D.N.C. 2020).

115. *Id.* at *8.

116. *Id.*

117. *Id. See also* United States v. Adkinson, 916 F.3d 605, 611 (7th Cir. 2019) ("[*Carpenter*] did not invalidate warrantless tower dumps (which identified phones near *one location* . . . at *one time* . . .) because the Supreme Court declined to rule that these dumps were searches requiring warrants.").

118. *See Carpenter*, 138 S. Ct. at 2217 (2018) (emphasizing the "intimate window" revealed by historical CSLI).

119. *Cf. Karo*, 468 U.S. at 715 (1984) (holding that accessing information from inside of a private residence is a search).

120. United States v. Lambis, 197 F. Supp. 3d 606, 609 (S.D.N.Y. 2016). *See also Cell-Site Simulators/IMSI Catchers*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/pages/cell-site-simulatorsimsi-catchers (summarizing these features) [https://perma.cc/N3F9-W5XY].

level crimes.[121] The *Katz* inquiry rarely comes up in cell-site simulator cases, perhaps because government agencies tend to get a warrant before using the device.[122]

Cell-site simulators share characteristics with tower dumps. Both receive data from a collective group of people at a single moment. Considering this location data collectively is irrelevant in a Fourth Amendment analysis—what matters is how the surveillance affected the individual defendant. But cell-site simulators still have intrusive characteristics. They can obtain individuals' locations through data that cell phones passively generate. Additionally, cell-site simulators can gather information about constitutionally protected places, like homes and places of worship. Courts have found arguments based on these characteristics persuasive.[123] For example, the court in *State v. Sylvestre*[124] held that using cell-site simulators is always a search.[125] It focused on the invasiveness of a cell-site simulator compared to historical CSLI, especially because cell phones can enter into "private residence[s]" and "other potentially revealing locales."[126] Even if the court did not consider the mosaic theory in its analysis, the *Sylvestre* court's focus on the nature of information obtained reflects *Carpenter*'s two-step approach.

C. GPS Location Data

GPS tracking devices have been around for decades—from the primitive GPS beeper in *Knotts* and *Karo* to the sophisticated version in *Jones*.[127] As the concurrences in *Jones* noted, GPS tracking devices provide detailed

121. Harvey Gee, *Almost Gone: The Vanishing Fourth Amendment's Allowance of Stingray Surveillance in a Post*-Carpenter *Age*, 28 REV. L. & SOC. JUST. 409, 432–33 (2019) (chronicling use of cell-site simulators).

122. *See* DEP'T OF JUST., DEPARTMENT OF JUSTICE POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY 3 (2015), https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators (requiring federal agents to obtain a search warrant prior to using a cell-site simulator) [https://perma.cc/4LLF-FA8Z]; DEP'T OF HOMELAND SEC., POLICY DIRECTIVE 047-02, DEPARTMENT POLICY REGARDING THE USE OF CELL-SITE SIMULATOR TECHNOLOGY 4 (2015), https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20 Use%20of%20Cell-Site%20Simulator%20Technology.pdf (same) [https://perma.cc/Z6ES-MFBR].

123. *See* State v. Martin, 287 So.3d 645, 648 (Fla. Ct. App. 2019) (holding use of a cell-site simulator to be a search because it "allows law enforcement to track an individual's location in real time"); *Sylvestre*, 254 So.3d at 991 (same). *But see* United States v. Woodson, 2018 WL 7150388, at *9 (E.D. Mo. Nov. 21, 2018) (distinguishing *Carpenter* because police were surveilling the suspect physically while using the cell-site simulator).

124. 254 So.3d 986 (Fla. Ct. App. 2018).

125. *Id.* at 991.

126. *Id.*

127. *Jones*, 565 U.S. at 403 (2012); *Karo*, 468 U.S. at 708 (1984); United States v. Knotts, 460 U.S. 276, 278 (1983).

location information about an individual over a span of time.[128] Lower courts have applied *Carpenter* to GPS data under both versions of the mosaic theory. In *United States v. Diggs*,[129] tracking the defendant "over the course of a month" was a search because of the "duration and level of the GPS data" in the specific case.[130] And in *Kinslow v. State*,[131] a state court found the use of a GPS tracker *not* to be a search because the tracking "lasted only approximately six hours" and because GPS data "[does] not provide an intimate window into a person's life."[132] In both these cases, the courts incorporated case facts when evaluating the nature of GPS location data.

United States v. Howard adopted the two-step mosaic inquiry, though, despite stating that its conclusion "[did] not rest on the mosaic theory."[133] Accessing GPS location data, the court reasoned, was not intrusive enough to violate a reasonable expectation of privacy. GPS location data does not allow police to "reconstruct a person's movements," nor does it follow people "into homes and other constitutionally protected spaces."[134] In addition to considering the overall nature of GPS data, the court evaluated the amount of data collected.[135] But its analysis of the nature of GPS data reflects the two-step mosaic theory—what the aggregated data could reveal when accessed.

D. Automated License Plate Readers (ALPRs)

ALPRs are video cameras connected to a central database that log the license plates in their field of vision, as well as the location, date, and time.[136] Because they can capture this time-stamped location information, ALPRs would seem analogous to the government's access of historical CSLI from *Carpenter*. ALPRs do only reveal information about people driving on public roadways. But enough ALPR data points could reveal patterns that become an "intimate window" into an individual's life.[137]

One group of cases has adopted the one-step mosaic inquiry—the amount of data is a factor when considering the nature of the information

128. *See* subpart II(B) (discussing *Jones*).

129. 385 F. Supp. 3d 648 (N.D. Ill. 2019).

130. *Id.* at 652.

131. 129 N.E.3d 810 (Ind. Ct. App. 2019) (unpublished table disposition).

132. *Id.* at *3 n.6; *see also Johnson*, 119 N.E.3d at 678–80 (recognizing that GPS monitoring enables "reconstruct[ing] a complete mapping of a probationer's movements" to discover "an extensive amount of sensitive and private information," but holding not to be a search because probationers have reduced expectations of privacy).

133. *Howard*, 426 F. Supp. 3d at 1256.

134. *Id.* at 1257 (citations omitted).

135. *Id.* at 1256–57.

136. *Automated License Plate Readers (ALPRs)*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/automated-license-plate-readers-alpr (Aug. 28, 2017) [https://perma.cc/V2UL-LQGN]; Kerr, *supra* note 56.

137. *See* Carpenter, 138 S. Ct. at 2217 (referring to this "intimate window").

obtained. The court in *Chaney v. City of Albany*[138] held that using "fixed cameras" that "indiscriminately recorded 24-hours a day" was not a search.[139] This specific use captured only information about people "traveling on public roads," and people have no reasonable expectation of privacy in this public space.[140] Similarly, the opinion in *Uhunmwangho v. State*[141] used the case facts to define the nature of the information obtained. Because police had retrieved "a single photograph" of the defendant "driving on a public roadway," the case did not raise the privacy concerns of *Carpenter*.[142]

Another line of cases has applied the two-step mosaic theory to ALPRs. Take *United States v. Yang*,[143] in which police queried an ALPR database to find a fugitive.[144] Though a Ninth Circuit panel declined to hold this query a search on standing grounds, Judge Carlos Bea wrote a concurrence reflecting the two-step mosaic theory.[145] ALPRs "*may* in time present many of the same issues" as in *Carpenter*, Judge Bea reasoned, as they can "effortlessly, and automatically, create voluminous databases of vehicle location information."[146] But even though ALPRs *could* violate a reasonable expectation of privacy, they did not do so in the present case—the database query "did not reveal the whole, or even any, of [the defendant's] physical movements."[147]

Commonwealth v. McCarthy also embraced the two-step mosaic inquiry of *Carpenter*. In the *McCarthy* court's view, "[a] detailed account of a person's movements, drawn from electronic surveillance," could violate a reasonable expectation of privacy because "the whole reveals far more than the sum of its parts."[148] If an ALPR system had "enough cameras in enough locations," then accessing it could be a search.[149] After establishing that the nature of ALPR data could violate the *Katz* standard, the court then turned to the facts of the case. Because the record indicated there were only "four cameras at fixed locations on the ends of two bridges"—basically, telling police

138. No. 6:16-CV-1185 (NAM/TWD), 2019 WL 3857995 (N.D.N.Y. Aug. 16, 2019).

139. *Id.* at *9.

140. *Id; cf. Knotts*, 460 U.S. at 281–82 (holding that a beeper radio transmitter monitoring a car on public roads is not a search).

141. No. 09-19-00119-CR, 2020 WL 1442640 (Tex. App.—Beaumont March 25, 2020, no pet.) (mem op., not designated for publication).

142. *Id.* at *8.

143. 958 F.3d 851 (9th Cir. 2020).

144. *Id.* at 854–55.

145. *Id.* at 861–62. Because the defendant's rental car was overdue, the court was "unwilling to conclude" that he had a reasonable expectation of privacy in the car's location data. *Id*.

146. *Id.* at 863 (Bea, J., concurring).

147. *Id.* at 864 (Bea, J., concurring).

148. *McCarthy*, 142 N.E.3d at 1103.

149. *Id.* at 1104.

when people entered or left Cape Cod—the court held that accessing this data was not a search.[150]

E. Video Surveillance and Pole Cameras

Carpenter has also led to challenges to long-term video surveillance. Specifically, pole cameras—fixed video cameras that police attach to utility poles. Pole cameras can record video continuously, can zoom, pan, and tilt, and can be operated remotely.[151] And they are not limited to surveillance of specific persons. Cities have begun creating video surveillance systems for public spaces as well.[152] Challenges to pole-camera surveillance reflect concerns over new video technology—drone cameras,[153] facial-recognition technology,[154] and software that can analyze "volumes of video that would otherwise be impossible."[155]

Pole cameras present a close case under the two-step mosaic inquiry. They record footage of people in public; not in their homes, their places of worship, or other constitutionally protected places.[156] Moreover, pole

150. *Id.* at 1106.

151. *See* United States v. Tuggle, No. 16-cr-20070-JES-JEH, 2018 WL 3631881, at *1 (C.D. Ill. July 31, 2018) (describing these features); United States v. Kay, 2018 WL 3995902, at *1 (E.D. Wis. Aug. 21, 2018) (same); *Surveillance Cameras*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/surveillance-cameras (Feb. 2, 2019) (same) [https://perma.cc/3WHC-SXDA].

152. *E.g.*, Daniel Rivero, *Miami Could Let Company Put Surveillance Poles On Public Property For Free*, WLRN 91.3 FM (Oct. 9, 2019), https://www.wlrn.org/local-news/2019-10-09/miami-could-let-company-put-surveillance-poles-on-public-property-for-free_ (discussing a proposal in Miami to allow a private company to place lighting and surveillance poles on public property); Sarah Holder, *In San Diego, 'Smart' Streetlights Spark Surveillance Reform*, BLOOMBERG CITYLAB (Aug. 6, 2020), https://www.bloomberg.com/news/articles/2020-08-06/a-surveillance-standoff-over-smart-streetlights (analyzing the implementation of San Diego's smart streetlight pilot program, which outifts streetlights with LEDs and small nodes that capture video) [https://perma.cc/ZLK9-ACJN].

153. Jason Koebler, *This Drone Zoom Lens Can Identify Your Face From 1,000 Feet Away*, VICE (Feb. 25, 2015), https://www.vice.com/en_us/article/8qxe93/this-drone-zoom-lens-can-identify-your-face-from-1000-feet-away [https://perma.cc/SP4P-GWDB].

154. *Face Recognition*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/face-recognition (Oct. 24, 2017) [https://perma.cc/M3VJ-N8QQ].

155. *Video Analytics Solutions for Post-Event Investigations*, BRIEFCAM, https://www.briefcam.com/solutions/police-investigations/ (last visited March 2, 2021) [https://perma.cc/JZ2L-KZPW].

156. *See* United States v. Moore-Bush, 963 F.3d 29, 42 (1st Cir. 2020) ("There is no equivalent analogy [between historical CSLI and] what is captured by the pole camera on the public street, which is taking images of public views and not more."), *reh'g en banc granted, opinion vacated*, 982 F.3d 50, 50 (1st Cir. 2020); United States v. Bronner, No. 3:19-cr-109-J-34JRK, 2020 WL 3491965, at *23 (M.D. Fla. May 18, 2020) (holding the use of a pole camera was not a search "notwithstanding the length of the surveillance . . . and the camera's capabilities"); United States v. Edmonds, 438 F. Supp. 3d 689 (S.D. W. Va. 2020) (holding not a search because the pole camera captured only "footage of vehicles coming and going from the residence," which "can be observed by any neighbor, passer-by, or officer"); *cf.* United States v. Kubasiak, No. 18-cr-120-pp, 2018 WL 4846761, at *7 (E.D. Wis. 2018) (holding use of a camera was not a search because it "recorded

cameras are not a technological innovation. They are, basically, security cameras—which the Supreme Court excluded from its holding in *Carpenter*.[157]

In *United States v. Moore-Bush*, for example, the district court applied the one-step mosaic inquiry, considering the nature of the surveillance in the specific case before it. Eight months of video data "captured every single second that passed . . . in a digitally searchable form," and could "[impair the defendants'] freedom to retreat" into their home.[158] Thus, the court held that the "intrusive, constant surveillance" over this eight months violated a reasonable expectation of privacy.[159] The First Circuit reversed.[160] A pole camera "tak[es] images of public views and not more," and "does not track the whole of a person's movement over time."[161] In the First Circuit's view, then, pole cameras could *never* violate a reasonable expectation of privacy by their very nature.[162] There was no need to address the facts of the specific case; the court disposed of the issue at the first step of the two-step mosaic theory.

In contrast, the court in *Commonwealth v. Mora* held that two months of pole-camera surveillance was a search, applying the two-step mosaic theory.[163] Though the court analyzed only a state constitution, it noted that the surveillance "well may have been a search" under the Fourth Amendment as well.[164] First, the court reasoned that "targeted long-term pole camera surveillance" of a residence "has the *capacity* to invade the security of the home."[165] Long-term surveillance "has the *potential*" to capture the "revealing interactions at the threshold of a person's private and public life."[166] After establishing that long-term pole-camera surveillance *could* violate a

only what the neighbor, or a police officer standing in the neighbor's house, could have seen"); United States v. Kelly, 385 F. Supp. 3d 721, 726 (E.D. Wis. 2019) (holding an apartment camera not a search because the camera could only see "what someone standing in the apartment hallway, or outside the apartment complex, could have seen").

157. *See Moore-Bush*, 963 F.3d at 40 ("Pole cameras are conventional, not new, technology."); United States v. Fanning, No. 1:18-cr-362-AT-CMS, 2019 WL 6462830, at *4 (N.D. Ga. May 28, 2019) (denying motion to suppress because pole cameras are "akin to a security camera," which *Carpenter* "expressly excluded from its holding").

158. United States v. Moore-Bush, 381 F. Supp. 3d 139, 149 (D. Mass. 2019), *rev'd*, 963 F.3d 29, 47 (1st Cir. 2020), *reh'g en banc granted, opinion vacated*, 982 F.3d 50, 50 (1st Cir. 2020).

159. *Id.* at 149–50.

160. *Moore-Bush*, 963 F.3d at 31.

161. *Id.* at 42.

162. *See id.* (noting that the Fourth Amendment has never "require[d] law enforcement officers to shield their eyes when passing by a home on public thoroughfares" (citing California v. Ciraolo, 476 U.S. 207, 213 (1986)).

163. *Mora*, 150 N.E.3d at 312–13.

164. *Id.* at 302.

165. *Id.* at 309 (emphasis added).

166. *Id.* at 311 (emphasis added).

reasonable expectation of privacy, the court applied the facts—five months and two months' surveillance of the defendants' homes sufficed to be a search.[167]

The reasoning in *Moore-Bush* and *Mora* could hold sway for other types of video surveillance as well. *Leaders of a Beautiful Struggle v. Baltimore Police Department* is a case about a city police department using airplanes to surveil citizens in public.[168] The district court held that this surveillance was not a search. It reasoned that the program "cannot produce a running log" of peoples' whereabouts; and because the surveillance would only occur for twelve hours a day, the "gaps in the data" would prevent long-term, continuous tracking.[169] Moreover, it only tracks people in public spaces—not their activities in the "home, shower . . . or daily sauna and bath."[170] But this reasoning overlooks that aggregated location data—as in *Carpenter*—can still paint a picture even if it is not continuous. Regardless, *Leaders* shows that these factors—location, duration, and continuous collection—could be dispositive in a two-step mosaic analysis.

F. Internet Protocol (IP) Address Data

Internet metadata provides another close case for applying *Carpenter*. The internet is, at bottom, a way for various devices to communicate with each other. To do so, computers and cell phones have internet protocol (IP) addresses—unique numbers that represent every device connected to the internet.[171] Internet service providers (ISPs) assign these addresses to users that purchase internet connections from them.[172] Because ISPs facilitate internet connections, they can collect data on the websites and content that users visit.[173] Collecting this user information could reveal intimate personal details, like what their personal hobbies, sexual orientation, or political beliefs are.[174]

Courts have been hesitant to hold that accessing IP address information is a search. Many apply the third-party doctrine because users must

167. *Id.* at 311–13.

168. 456 F. Supp. 3d at 702–03.

169. *Id.* at 715–17 (citations omitted).

170. *Id.* (internal quotations omitted).

171. ICANN, BEGINNER'S GUIDE TO INTERNET PROTOCOL (IP) ADDRESSES 2 (2011), https://www.icann.org/en/system/files/files/ip-addresses-beginners-guide-04mar11-en.pdf [https://perma.cc/WU86-43UT].

172. Travis Panneck, Note, *Incognito Mode is in the Constitution*, 104 MINN. L. REV. 511, 515 (2019).

173. Aaron Rieke, David Robinson, & Harlan Yu, *What ISPs Can See*, UPTURN (Mar. 2016), https://www.upturn.org/reports/2016/what-isps-can-see/ [https://perma.cc/T2YH-47AN].

174. *See* Kerr, *supra* note 2, at 47 (describing these concerns); Panneck, *supra* note 172, at 518.

affirmatively act to generate IP address data.[175] This rationale follows pre-*Carpenter* decisions holding the same.[176] Other courts distinguish IP address data because it does not track a user's location.[177] These courts' reasoning adheres to the two-step mosaic theory—it focuses on what aggregated IP address data *could* reveal rather than what it *does* reveal in the present case. For example, in *United States v. Hood*, the First Circuit considered the nature of IP address information to be dispositive. IP address data "does not itself convey any location information" and requires an "affirmative decision" by the user.[178] And in *United States v. Monroe*, the court reasoned that IP address data "does not, in and of itself, reveal a particular user's identity or the content of the user's communications."[179]

Against this trend, the Southern District of New York has indicated receptiveness to requiring a warrant to access IP address data. In *United States v. Kidd*,[180] agents had subpoenaed 581 days and "nearly 1,800 pages" of IP address data from a cell phone.[181] First, the court considered the nature of IP address information, reasoning that it "*may convey* location information with similar degrees of specificity . . . as CSLI does."[182] "Passive collection of IP address information" could violate a reasonable expectation of privacy, but

175. *See, e.g.*, United States v. Trader, 981 F.3d 961, 968 (11th Cir. 2020) (holding that the third-party doctrine applied to a criminal suspect's email and IP addresses); United States v. Hood, 920 F.3d 87, 92 (1st Cir. 2019) (reasoning that internet users generate IP address data "only by making the affirmative decision to access a website or application"); United States v. Contreras, 905 F.3d 853, 857 (5th Cir. 2018) (holding the information fell "comfortably within the scope of the third-party doctrine"); United States v. Rosenow, Case No. 17CR3430 WQH, 2018 WL 6064949, at *11 (S.D. Cal. Nov. 20, 2018) (not a search because defendant "voluntarily provided" it to ISPs); United States v. Felton, 67 F. Supp. 3d 569, 575 (W.D. La. 2019) (rejecting claim because of third-party doctrine); United States v. Tolbert, No. 14-3761 JCH, 2019 WL 2006464, at *3 (D.N.M. May 7, 2019) (noting the "affirmative actions" of the defendant in generating IP address data); United States v. Cox, No. 1:18-CR-83-HAB, 2020 WL 2899685, at *4 (N.D. Ind. June 3, 2020) (holding that IP address data fits "comfortably" within the third-party doctrine).

176. *E.g.*, United States v. Ulbricht, 858 F.3d 71, 96–97 (2d Cir. 2017); United States v. Wheelock, 772 F.3d 825, 828 (8th Cir. 2014); United States v. Christie, 624 F.3d 558, 574 (3d Cir. 2010); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007).

177. *See, e.g.*, United States v. Monroe, 350 F. Supp. 3d 43, 49 (D.R.I. 2018) ("[An IP address] does not reveal the kind of minutely detailed, historical portrait . . . that concerned the Supreme Court in *Carpenter* . . . ."); *Hood*, 920 F.3d at 92 (noting that IP address data "does not itself convey any location information"); United States v. Jenkins, No. 1:18-cr-00181, 2019 WL 1568154, at *4 (N.D. Ga. Apr. 11, 2019) (same); United States v. McCutchin, No. CR-17-01517-001-TUC-JAS (BPV), 2019 WL 1075544, at *2 (D. Ariz. Mar. 7, 2019) (reasoning that IP address data does not reveal "familial, political, professional, religious, sexual associations, or location"); United States v. Germain, Case No. 2:18-cr-00026, 2019 WL 1970779, at *4 (D. Vt. May 3, 2019) (rejecting claim because IP address data "does not reveal [d]efendant's physical movements or the location of his cell phone"); *Tolbert*, 2019 WL 2006464, at *3 (same).

178. *Hood*, 920 F.3d at 92.

179. *Monroe*, 350 F. Supp. 3d at 48.

180. 394 F. Supp. 3d 357 (S.D.N.Y. 2019).

181. *Id.* at 368.

182. *Id.* at 365.

only if it "provides geographically accurate information that follows a defendant's day-to-day movements."[183] Since the defendant had failed to include facts about this issue in the record, the court denied his motion to suppress.[184] But it cautioned against the "categorical approach" of the post-*Carpenter* cases involving IP addresses—especially with respect to the amount of data involved.[185] Similarly, in *United States v. Hernandez*,[186] the court accepted *Kidd*'s reasoning that IP address information could violate a reasonable expectation of privacy. But because the data in the case contained "significantly fewer data points" than in *Carpenter*, and because the facts did not indicate that the data conveyed "geographically accurate information," the court denied the defendant's motion to suppress.[187] In both *Kidd* and *Hernandez*, the courts reasoned that IP address data *could* violate a reasonable expectation of privacy. The data in the present cases just did not reach that potential.

G. "Smart" Devices and the "Internet of Things"

"Smart" devices are ordinary objects that can communicate data over the internet.[188] Together, they make up the "Internet of Things" (IOT)—a network of once-ordinary devices communicating data with each other over the internet.[189] Because smart devices are quickly becoming pervasive in homes,[190] the large quantities of data they produce raises privacy concerns. So, in *Naperville Smart Meter Awareness v. City of Naperville*, [191] the Seventh Circuit held that the use of "smart meters" that recorded homes' energy consumption every fifteen minutes was a search.[192] But the court in *Naperville* did not adopt either mosaic theory—rather, the court considered only the nature of the information that smart meters provided. Data on energy consumption, the court reasoned, can indicate "when people are home, when people are away, [and] when people sleep and eat," among other

183. *Id.* at 367.

184. *Id.* at 368.

185. *Id.* at 368.

186. 2020 WL 3257937 (S.D.N.Y. June 16, 2020).

187. *Id.* at *20–21.

188. Gabriel Bronshteyn, Note, *Searching the Smart Home*, 72 STAN. L. REV. 455, 459–60 (2020).

189. *Id.*

190. *See Smart Speaker Consumer Adoption Report*, VOICEBOT (March 2019), https://voicebot.ai/wp-content/uploads/2019/03/smart_speaker_consumer_adoption_report_2019.pdf (finding that 26.2% of all U.S. adults owned smart speakers as of March 2019) [https://perma.cc/43D9-NU74].

191. 900 F.3d 521 (7th Cir. 2018).

192. *Id.* at 524, 527.

information.[193] Because this recordkeeping "reveal[ed] details about the home" that agents could not see otherwise, it was a search.[194]

H. Other Types of Digital Data

Because of *Carpenter*'s sweeping language, courts have faced Fourth Amendment challenges to acquisition of data in a variety of other contexts. Peer-to-peer file-sharing networks,[195] cryptocurrency transactions,[196] and social media posts,[197] among others. These cases tend to reject analogies to *Carpenter* based on the nature of the data involved. The court in *United States v. Sigouin* distinguished peer-to-peer networks because the data "communicates nothing" about the file's content or the sender's information.[198] In *United States v. Gratkowski*, the court emphasized that cryptocurrency ledgers convey "limited" information, require an affirmative act, and are publicly available.[199] And in *United States v. Chavez*, the court held that accessing nonpublic Facebook data was always a search because the information could "create a 'revealing montage of the user's life.'"[200] Though these courts did not consider the amount of information—*i.e.*, neither mosaic theory—they accept *Carpenter*'s shift in focus to the nature of information conveyed. Courts should consider what the information could potentially reveal prior to considering what the information in the case actually revealed.

III. Reviewing the Mosaic Theories

If anything, this review of lower-court decisions demonstrates the incoherence of the mosaic theory as a reasoning tool. The doctrine surrounding

193. *Id.* at 526.

194. *Id.* at 527.

195. *E.g.*, United States v. Shipton, No. 0:18-cr-202-PJS-KMM, 2019 WL 5330928, at *16 (D. Minn. 2019) (holding not a search because the data is "something that [defendant] chose not to keep private"); United States v. Sigouin, NO. 9:19-CR-80136-ROSENBERG/REINHART, 2019 WL 7372958, at *6 (S.D. Fla. Dec. 19, 2019) (holding no search occurred because the "hash value" in a P2P file communicates "nothing . . . about the sender" other than a desire to retrieve a file).

196. *E.g.*, United States v. Gratkowski, 964 F.3d 307, 310 (5th Cir. 2020) (holding that one has no expectation of privacy in information on a blockchain or a virtual currency exchange); Zietzke v. United States (*Zietzke II*), No. 19-cv-03761-HSG(SK), 2020 WL 264394, at *13 (N.D. Cal. Jan. 17, 2020) (holding no expectation of privacy in Bitcoin transaction records); Zietzke v. United States (*Zietzke I*), 426 F. Supp. 3d 758, 768–69 (W.D. Wash. 2019) (same).

197. *E.g.*, United States v. Westley, No. 3:17-CR-171 (MPS), 2018 WL 3448161, at *14 n.9 (D. Conn. July 17, 2018) (holding that data provided to Facebook falls within the third-party doctrine); United States v. Chavez, 423 F. Supp. 3d 194, 203–04 (W.D.N.C. 2019) (holding that obtaining nonpublic Facebook information constitutes a search because it may reveal "intimate, momentous, and sometimes weighty information").

198. *Sigouin*, 2019 WL 7372958, at *7.

199. *Gratkowski*, 964 F.3d at 310.

200. *Chavez*, 423 F. Supp. 3d at 204 (citing Riley v. California, 134 S. Ct. 2473, 2490 (2014)).

the Fourth Amendment's search requirement should be focused on drawing lines for law enforcement. After all, any of the above-mentioned cases would not have been at issue had the police gotten a warrant. The one-step mosaic theory undermines this rationale. Courts applying the one-step approach draw lines around the amount of information obtained, rather than the nature of the information itself. These decisions threaten to ossify Fourth Amendment doctrine through precedential decisions on categories of surveillance, with reasoning based on case-specific facts. In this regard, the two-step mosaic theory has advantages over its one-step counterpart. Digital data encompasses a wide spectrum of different types of information, and the modes of digital surveillance are changing by the day. By applying the new mosaic theory, judges can resolve the disputes in front of them while leaving the door open for future technological developments—exactly what the Court did in *Carpenter*. Additionally, the new mosaic theory would provide an avenue to transition the mosaic theory into a truly categorical approach to data. If a lower court holds that accessing *any* amount would violate a reasonable expectation of privacy, then it has both adhered to *Carpenter*'s new mosaic theory while creating a bright-line rule for law enforcement to follow.

A. Drawing Lines Based on Type of Information

First, lower courts have centered the *Carpenter* analysis around the nature of information conveyed. If the digital data in the case does not reveal information about the "privacies of life," then it should not be considered a search. This standard does lead to problems—namely, when should the amount of data factor in? Professor Ohm, for example, interprets *Carpenter* to require a one-step analysis, with the amount of information in the case being a factor.[201] This Note has argued that *Carpenter* separates this analysis into two steps. When considering the nature of information conveyed by data, courts should ask whether that data could violate a reasonable expectation of privacy when aggregated. Only then should they consider the amount of data in the case. In the en banc rehearing of *Moore-Bush*, counsel for the ACLU advocated for a line-drawing in a similar manner:

> I think that if this court wishes to draw a line, or a principle, it should be tied to what people's expectation is, based on the practical abilities of police and any member of the public. People expect and understand that their activities in public, including in the curtilage of their home, may be observed in bits and pieces. Nobody

201. Ohm, *supra* note 4, at 373 (arguing that *Carpenter*'s identification of "comprehensive reach" as a factor "in effect endorses the mosaic theory of privacy").

> expects the whole of those movements, over a long period, to be seen and recorded.[202]

Several lower courts that have engaged with the mosaic theory have adopted similar two-step approaches.[203]

By providing a two-step process, the new mosaic theory allows lower courts to draw lines based on the type of information obtained by law enforcement. When facing a new kind of technology, courts can analogize to past technologies when assessing its nature. This process allows courts, effectively, to declare law about certain types of surveillance while still allowing case-by-case evaluation. Consider *Commonwealth v. McCarthy*, in which the court reasoned that an ALPR system could potentially violate a reasonable expectation of privacy.[204] Though the ALPR system did not reach that level in *McCarthy*, the court's reasoning stands ready in case the system eventually does. This process will provide increased accuracy and certainty when lower courts conduct a reasonable-expectation-of-privacy analysis.[205]

Recognizing the two different mosaic theories also allows lower courts to be explicit about which test they are applying. The new mosaic theory has two steps: *Carpenter* applied a multifactor test, but only at the first step (when considering the nature of information). Moreover, *Carpenter* waited to apply case facts until after assessing the nature of data obtained. Incorporating case facts into the first step clouds the common law—reasoning by analogy is far harder when the factors are case-specific.[206]

B. The New Mosaic Theory Allows for a Categorical Approach

Second, lower courts are divided over whether *Carpenter* mandates a categorical approach to digital data or a case-by-case analysis. The courts applying either mosaic theory have accepted a case-by-case approach.[207]

---

202. Oral Argument at 1:13:30, United States v. Moore-Bush (1st Cir. Mar. 23, 2021) (No. 19-1582) (en banc) (argument of ACLU as *amicus curiae*), http://media.ca1.uscourts.gov/files/audio/19-1582.mp3.

203. *See, e.g.*, United States v. Yang, 958 F.3d 851, 863–64 (9th Cir. 2020) (Bea, J., concurring in the judgment) (analyzing the potential of ALPR cameras to violate an expectation of privacy before applying the facts of the case); *McCarthy*, 142 N.E.3d at 1104–05 (considering the amount of ALPR cameras in the case only after assessing ALPRs' potential to invade on privacy).

204. *McCarthy*, 142 N.E.3d at 1103.

205. *See Hood*, 920 F.3d at 92 (holding that accessing IP address data is never a search because it is generated by an affirmative act of the user); *cf.* Kerr, *supra* note 16, at 546 (noting that lower courts' choice between models allows for this same consistency).

206. *Compare Uhunmwangho* 2020 WL 1442640, at *8 (holding that a single ALPR photograph did not raise the privacy concerns of *Carpenter*), *with Yang*, 958 F.3d at 863 (Bea, J., concurring) (reasoning that ALPRs could raise the privacy concerns of *Carpenter* because they can "effortlessly, and automatically, create voluminous databases of vehicle location information").

207. *See McCarthy*, 142 N.E.3d at 1105 (assessing the "constitutional import" of "four cameras placed at two fixed locations"); Sims v. State, 569 N.W.3d 634, 646 (Tex. Crim. App. 2019)

Other courts identify this concern and reject a case-by-case analysis altogether.[208] This analysis differs based on the type of mosaic theory applied. Under the one-step mosaic theory, case-by-case analysis is mandatory. It is the amount of data *in the present case* that factors into the *Katz* analysis. The two-step mosaic theory differs.

Because the two-step mosaic theory asks what information aggregated data could reveal, it provides an off-ramp for courts wishing to draw bright-line rules. As the Court itself said: "It is sufficient for our purposes . . . to hold that accessing seven days of CSLI constitutes a Fourth Amendment search."[209] The court cast no judgment on whether a smaller amount of CSLI would be a search—rather, it simply applied the facts of the case to the determination that historical CSLI *could* violate a reasonable expectation of privacy.[210] Nothing about *Carpenter* or the new mosaic theory prevents courts from holding that accessing *any* amount of a certain type of data would be a search.

Several courts have, accordingly, applied *Carpenter*'s two-step process while holding that accessing a type of data is always a search. Consider *Naperville Smart Meter Awareness*—because data from smart meters "reveal[ed] details about the home," accessing any amount of that data would be a search.[211] In *United States v. Chavez*, as well, the court reasoned that non-public Facebook information could create a "revealing montage" of a user's private details.[212] Because this information is so private, accessing any amount would violate a reasonable expectation of privacy. And in *Muhammad*, the court engaged in a two-step process. After finding that real-time CSLI could violate a reasonable expectation of privacy, the court then applied its finding to real-time CSLI generally.[213] But if it had incorporated the amount of data into its analysis of real-time CSLI's nature, this reasoning would not be possible.

This reading of the new mosaic theory arguably may not reflect the "mosaic" concept at all. If even a single piece of information could reveal one's privacies of life, then it is less like a mosaic and more like a Rothko

("Whether a person has a recognized expectation of privacy in real-time CSLI records must be decided on a case-by-case basis.").

208. *See Muhammad*, 451 P.3d at 1072 (holding access of real-time CSLI is always a search). *See also Kidd*, 394 F. Supp. 3d at 368 (noting the categorical approach courts have applied to cases involving IP address data).

209. *Carpenter*, 138 S. Ct. at 2217 n.3..

210. *See id.* at 2212 (explaining that the government's smallest request for historical CSLI was a request for seven days' worth from Sprint).

211. *Naperville Smart Meter Awareness*, 900 F.3d at 527.

212. *Chavez*, 423 F. Supp. 3d at 203.

213. *Muhammad*, 451 P.3d at 1071–72.

painting.[214] But this concept reflects the importance of the shift in *Carpenter*. By separating out the application of case facts, the Court in *Carpenter* reframed the mosaic theory to better allow courts to draw normative considerations. It allowed for equilibrium-adjustment between police power and individual privacy while incorporating the concept of aggregated digital data. And it enabled lower courts to draw lines, even categorical ones, if the normative considerations bear enough weight. In short, recognizing the new mosaic theory would promote consistency and efficient equilibrium-adjustment in the lower courts. And applying a categorical approach through the two-step mosaic theory provides a means to do so.

IV. Conclusion

Digital data has become ubiquitous in our daily lives. *Carpenter*'s two-step mosaic theory provides one way of assessing this data—and it does so better than *Jones*'s one-step process. An analysis of lower court decisions shows that they have largely adopted this two-step approach: considering the type of information revealed, then applying the facts of the case. Finally, *Carpenter*'s two-step process has several benefits over the one-step mosaic theory. It allows courts to provide reasoning about why certain information should be protected or not. It prevents ossification of Fourth Amendment doctrine in the rapidly changing field of digital surveillance. And it provides a doctrinal means to incorporate policy factors when considering digital data.

214. *See Mark Rothko: Classic Paintings*, NATIONAL GALLERY OF ART, https://www.nga.gov/features/mark-rothko/mark-rothko-classic-paintings.html (showing large compositions of a single color) [https://perma.cc/3ZNQ-5T3V].