APPLYING THE EXCLUSIONARY RULE TO *CARPENTER* SEARCHES

KEVIN GANLEY*

TABLE OF CONTENTS

*. Editor-in-Chief, *Southern California Law Review*, Volume 93; J.D. Candidate 2020, University of Southern California, Gould School of Law; B.B.A. Finance 2017, University of San Diego; B.A. Political Science 2017, University of San Diego. I would like to thank my Mom, my Dad, Matt, and Madeline for their love and support throughout my time in law school. I would also like to thank Professor Sam Erman for his guidance as I worked through the many versions of this Note as well Professor Orin Kerr for his feedback on my manuscript. Finally, I would like to thank the talented members of the *Southern California Law Review* for their excellent editing work.

INTRODUCTION

People unwittingly divulge substantial sums of personal information to third-party businesses. Many of these businesses, in turn, compile and aggregate this information as a matter of profit.[1] For example, Amazon, Facebook, and Google automatically collect and store their users' personal information and browsing histories to improve user experience and advertisement effectiveness.[2] Wireless carriers retain their users' cell-site location information ("CSLI"), functionally allowing them to track their users' daily movements, in order to manage cell tower traffic and improve service.[3] Often, consumers benefit from these transactions in a narrow sense, but the resultant surveillance capacities that companies develop in doing so eerily parallel those of "Big Brother" in George Orwell's famous novel, *1984*.[4]

What is perhaps most unnerving is that prior to the Supreme Court's June 2018 ruling in *Carpenter v. United States*,[5] the government could access all of this digital information without a warrant.[6] Under the Fourth Amendment's third-party doctrine, people did not have a constitutionally protected expectation of privacy in this digital user information if they "voluntarily" conveyed it to third-party companies.[7]

1. *See* Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 817 (2016) ("Mapping consumer interests at an extremely personal level has become a growing and quite lucrative business, with many big technology companies jumping into the field.").

2. *Amazon Privacy Notice*, AMAZON (Jan. 1, 2020), https://www.amazon.com/gp/help/customer/display.html?nodeId=201909010#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_467C686A137847768F44B619694D3F7C [https://perma.cc/S9QE-GD9C]; *Google Privacy Policy*, GOOGLE (Mar. 31, 2020), https://www.gstatic.com/policies/privacy/pdf/20200331/acec359e/google_privacy_policy_en_us.pdf [https://perma.cc/UL7U-PZEP]; *How Does Facebook Decide Which Ads to Show Me?*, FACEBOOK HELP CTR., https://www.facebook.com/help/562973647153813 [https://perma.cc/H6A3-WU8C].

3. Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

4. *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 175–77 (2004) (discussing the "Orwellian" dangers presented by the information age and the third-party doctrine). For George Orwell's famous novel, see generally GEORGE ORWELL, 1984 (Houghton Mifflin Harcourt 2017) (1949) (depicting Big Brother as a fictional party leader in a totalitarian state who constantly surveils each citizen).

5. *Carpenter*, 138 S. Ct. at 2206.

6. *See id.* at 2213, 2217 (reversing a lower court decision that held no search occurred when the government accessed 127 days of CSLI).

7. *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 526 (2006) (citation omitted). For a deeper discussion of the vast power the third-party doctrine affords the government in the digital age, see generally Ian Samuel, *The New Writs of Assistance*, 86 FORDHAM L. REV. 2873 (2018) (arguing that network-connected digital devices have the potential to provide the government with near-perfect knowledge of people's daily lives); Ian James Samuel, Note, *Warrantless Location Tracking*, 83

Specifically, *Carpenter* dealt with whether the government needed a warrant to subpoena 127 days' worth of CSLI from a defendant's wireless carriers—which allowed the government to roughly track the defendant's general movements over the requested time frame.[8] Side-stepping the third-party doctrine along the way,[9] the Court narrowly held that a government request for at least seven days of CSLI was "sufficient" to "constitute[] a Fourth Amendment search."[10]

In a broader sense, however, the *Carpenter* Court grappled with how to create new rules to defend privacy rights from government encroachment in the digital age.[11] Writing for the majority, Chief Justice Roberts relied heavily on broad, commonsense privacy notions to pivot away from the third-party doctrine.[12] In short, the Court required a warrant for long-term searches of CSLI to safeguard "the privacies of life" against the "arbitrary power"[13] the government acquired in the wake of recent "seismic" changes in technology.[14]

On its face, *Carpenter*'s message has intuitive appeal: the old rules should not apply because the Court's analog-search precedents may not adequately protect privacy rights in a digital world.[15] After all, if the Court were to hold otherwise, the government could digitally track its citizens by requesting access to large caches of third-party metadata without triggering

N.Y.U. L. REV. 1324 (2008) (discussing how the police track suspects using cell phones). For more on the third-party doctrine, see *infra* Section I.B.

8. *Carpenter*, 138 S. Ct. at 2211–12.

9. *Id.* at 2216–17 (declining to extend the third-party doctrine).

10. *Id.* at 2217 n.3.

11. ORIN S. KERR, *Implementing* Carpenter, *in* THE DIGITAL FOURTH AMENDMENT (forthcoming) [hereinafter KERR, *Implementing* Carpenter] (manuscript at 1–2) (on file with author). Legislatures worldwide are also creating new rules to address their constituents' digital privacy concerns. *See, e.g.*, Adam Satariano, *What the G.D.P.R., Europe's Tough New Data Law, Means for You*, N.Y. TIMES (May 6, 2018), https://www.nytimes.com/2018/05/06/technology/gdpr-european-privacy-law.html [https://perma.cc/JB57-MZWG] (discussing Europe's new digital privacy legislation); Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (June 28, 2018), https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html [https://perma.cc/JR76-PSY4] (discussing California's new internet privacy legislation).

12. *Carpenter*, 138 S. Ct. at 2217–20.

13. *Id.* at 2214.

14. *Id.* at 2219–20.

15. *See* Orin Kerr, *Understanding the Supreme Court's* Carpenter *Decision*, LAWFARE (June 22, 2018, 1:18 PM), https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision [https://perma.cc/KB3J-2B72] ("Throughout [*Carpenter*, Chief Justice Roberts] roots his analysis in the idea that cell-site surveillance is a new tool that gives the government new power that can be abused, and that the law must change course to ensure that the government doesn't get too much power from a mechanical application of the old rules.").

Fourth Amendment concerns.[16] Unfortunately, despite taking a step toward vindicating looming digital privacy concerns within Fourth Amendment jurisprudence, *Carpenter* left a lot to be desired.[17]

A fundamental question left unanswered by *Carpenter* is when a government request for digital metadata becomes a Fourth Amendment search. It is currently unclear whether the Court will focus in on rules governing the *quality* or *quantity* of digital information accessed by the government.[18] Orin Kerr advocates for the source rule, which focuses on the quality of the information that the government is seeking to access and holds that the government needs a warrant to access any digital information similar to CSLI,[19] regardless of how much digital information is actually obtained.[20]

On the other hand, the Court has also entertained the implementation of the mosaic theory.[21] This theory provides that the aggregation of digital records can invade someone's reasonable expectation of privacy, and thus constitute a Fourth Amendment search, even if the government's access to

16. *See* United States v. Carpenter, 819 F.3d 880, 884 (6th Cir. 2016), *rev'd*, 138 S. Ct. 2206 (2018).

17. *See* KERR, *Implementing* Carpenter, *supra* note 11 (manuscript at 1–3); Paul Rosenzweig, Carpenter v. United States *and the Law of the Chancellor's Foot*, LAWFARE (June 27, 2018, 7:41 AM), https://www.lawfareblog.com/carpenter-v-united-states-and-law-chancellors-foot [https://perma.cc/K549-7Q77] ("[T]he Supreme Court's decision in *Carpenter v. United States* is not law. Anyone who says they can read the majority opinion and predict with any degree of confidence how the Court will deal with any number of future technologies . . . is, frankly, just making it up."); Nathaniel Sobel, *Four Months Later, How Are Courts Interpreting* Carpenter*?*, LAWFARE (Oct. 18, 2018, 8:57 AM), https://www.lawfareblog.com/four-months-later-how-are-courts-interpreting-carpenter [https://perma.cc/SAE8-NWLC].

18. *See* KERR, *Implementing* Carpenter, *supra* note 11 (manuscript at 27–28) (taking the position that the Court should hold that the acquisition of any information subject to *Carpenter* requires a warrant); *see also Carpenter*, 138 S. Ct. at 2217 n.3 ("[W]e need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.").

19. The question of what other information can be likened to CSLI was left open by *Carpenter*. KERR, *Implementing* Carpenter, *supra* note 11 (manuscript at 2–3). Kerr thinks that *Carpenter* applies to records that (1) were only "made widely possible by surveillance methods of the digital age," (2) are "not . . . the product of a user's meaningful voluntary choice," and (3) "tend[] to reveal an intimate portrait of a person's life beyond the legitimate interests of criminal investigations." *Id.* (manuscript at 3). This analysis, however, is beyond the scope of this Note.

20. *Id.* (manuscript at 27–28).

21. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012); *see also Carpenter*, 138 S. Ct. at 2215, 2217–18 (explaining that five concurring justices in *United States v. Jones*, 565 U.S. 400 (2012), "concluded that longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy—regardless of whether those movements were disclosed to the public at large" (internal quotation marks omitted)).

each discrete datum is constitutionally non-invasive.[22] The problem with the mosaic theory is that it is hard to delineate when the government's acquisition of digital information becomes invasive enough to require a warrant.[23] This makes the mosaic theory difficult to administer, as it would require courts to engage in messy line-drawing while navigating additional doctrinal trouble spots.[24]

One of these trouble spots is the focus of this Note: whether and how to apply the exclusionary rule to a mosaic search violation.[25] Consider the following fictional example. The government subpoenaed ten days of CSLI to track a defendant's movements over that period, and a court, for the first time, holds that a mosaic "search" definitively occurred on day seven. Should all the information gathered be excluded from the defendant's trial under what this Note terms the "all-or-nothing approach"? Or should only the final three days of CSLI be excluded, leaving the government with the seven days of information that could have been obtained legally, under what this Note terms the "after-search approach"?

Unfortunately, both approaches are morbidly flawed. The all-or-nothing approach will over-deter the government by excluding evidence that the government could have constitutionally accessed if it had simply narrowed its request in the first place.[26] At the other extreme, the after-search approach incentivizes the government to make broad requests to ensure that

22. KERR, *Implementing* Carpenter, *supra* note 11 (manuscript at 35–36); Steven M. Bellovin et al., *When Enough Is Enough: Location Tracking, Mosaic Theory, and Machine Learning*, 8 N.Y.U. J.L. & LIBERTY 555, 556–57 (2014).

23. Kerr, *supra* note 21, at 333. *Cf.* Paul Rosenzweig, *In Defense of the Mosaic Theory*, LAWFARE (Nov. 29, 2017, 3:18 PM), https://www.lawfareblog.com/defense-mosaic-theory [https://perma.cc/LR53-P3FJ] (agreeing that the mosaic theory is flawed but arguing that it is the best possible approach).

24. KERR, *Implementing* Carpenter, *supra* note 11 (manuscript at 27–28); David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 71 (2013) ("The best solution that mosaic advocates have . . . is to draw bright, if arbitrary, lines based on how long officers use an investigative method or technology. These kinds of solutions fail to satisfy because they are under inclusive, over inclusive, and also sidestep important conceptual and doctrinal questions." (footnote omitted)) (ultimately proposing a statutory solution similar to Kerr's source rule); Kerr, *supra* note 21, at 333.

25. Although it is ultimately a remedy question, it is prudent to look to the exclusionary rule first. After all, without the exclusionary rule, any mosaic search doctrine the Court prescribes would be "reduced to 'a form of words.' " Mapp v. Ohio, 367 U.S. 643, 648, 655 (1961) (quoting Silverthorne Lumber Co. v. United States, 251 U.S. 385, 392 (1920) (Holmes, J.)).

26. Using the previous fictional example, because the government searched more than seven days of CSLI, it would not be able to admit the CSLI at trial under the all-or-nothing approach. The problem is that the government would have been able to use the first seven days of information if the government had better guessed when the mosaic threshold would be triggered and limited its subpoena request accordingly.

it does not leave any digital evidence on the table.[27]

Considering the pitfalls of these approaches, this Note suggests an alternative middle ground—the "after-act approach." It requires only the exclusion of digital evidence gathered by the *single government act* that crossed the mosaic search threshold and any subsequent act also beyond this threshold. In the preceding example, all ten days of digital information would be excluded under this approach because there was only one act, the ten-day subpoena request. For this very reason, the after-act approach would incentivize government officers to break up their subpoenas for CSLI ex ante. Following the same example, if the after-act approach were employed, the government would be motivated to first subpoena only a few days of CSLI, giving it a narrower view of the defendant's travels, without triggering Fourth Amendment concerns, before subpoenaing the remaining days in the relevant time frame. This is because the evidence obtained by any subpoena before the mosaic threshold was crossed would still be admissible at trial. This accordingly creates various decision points in digital investigations that structure the inflow of evidence sequentially, facilitating judicial review and forcing government officers to be more conscious of their decisions to gather digital information without a warrant.

Thus, this Note is useful in two respects. First and foremost, it provides a plausible approach for applying the exclusionary rule to mosaic searches, removing a thorny obstacle in the mosaic theory's path. The after-act approach is also court friendly because it facilitates judicial review by incentivizing the government to show its work through sequencing its actions.[28] Second and more subtly, this Note may encourage courts to avoid the mosaic theory altogether. The Supreme Court's Fourth Amendment jurisprudence was already a "mess" before the digital age.[29] This Note describes several complicated doctrinal puzzles that arise at the intersection of the exclusionary rule and the mosaic theory. Adopting the bright-line

27. Under the after-search approach, if the government wanted to guarantee that it got all of the digital information it possibly could on any given suspect, it would make a broad request and wait for the reviewing court to delineate when the search occurred.

28. One of the knocks on the mosaic approach is that it does not fit neatly within the Court's existing Fourth Amendment doctrine which applies a sequential analysis to determining when a search occurs. *See infra* Section II.B. The after-act approach, however, incentivizes the government to create decision points in its digital searches, creating an artificial sequence to the inflow of evidence that makes it easier for courts to point to exactly when the search occurred within the scope of a digital investigation. *See infra* Section III.C.

29. Roger B. Dworkin, *Fact Style Adjudication and the Fourth Amendment: The Limits of Lawyering*, 48 IND. L.J. 329, 329 (1973).

source rule would avoid having to address these difficulties.[30]

Part I of this Note paints the backdrop underlying the *Carpenter* decision. It tracks the development of the Fourth Amendment search doctrine to the digital age and then demonstrates that over time the Court has adapted this doctrine in response to improvements in government surveillance technology.[31] Then, Part I explains how the Court's current analog-search rules, namely the third-party doctrine, have become outdated in the digital age.

Next, Part II of this Note explains how *Carpenter* marked a shift in the Court's understanding of its Fourth Amendment search doctrine in the digital age but left open how to determine when exactly a *Carpenter* search occurs on new sets of facts. It will then more thoroughly introduce the mosaic theory and the source rule, which are two possible methods for determining when a *Carpenter* search occurs. In comparing the relative merits of each method, Part II will explain that, although the mosaic theory is theoretically sound, its application to the Court's existing search doctrine presents many messy legal issues, including how to apply the exclusionary rule.

Part III addresses how to apply the exclusionary rule when a mosaic search occurs. In doing so, it briefly will introduce the exclusionary rule. It will then discuss the respective failings of the all-or-nothing and after-search approaches. Finally, Part III will outline the after-act approach and explain its various virtues, using the all-or-nothing and after-search approaches as foils.

I. TECHNOLOGY AND THE FOURTH AMENDMENT

Textually, the Fourth Amendment guarantees people the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[32] To protect these rights, the Fourth Amendment provides a procedural requirement that "no [w]arrants shall issue, but upon probable cause, supported by [o]ath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[33]

Section I.A will demonstrate that, over time, technological advancements have pushed the Court to think more deeply about what it

30. This Note will discuss the merits of the source rule and mosaic theory, *see infra* Section II.B, but it will not address which is ultimately preferable.

31. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 481–82 (2011).

32. U.S. CONST. amend. IV.

33. *Id.*

means to search and seize. In the mid-twentieth century, to combat new surveillance technologies, the Court expanded its search doctrine to protect people's reasonable expectations of privacy, rather than just their persons and property.[34] The Court was then tasked with defining what constitutes a reasonable expectation of privacy.[35] In doing so, it explicated the third-party doctrine, holding that people cannot have a reasonable expectation of privacy in the information they conveyed to third parties.[36]

Privacy issues generated as a result of the digital age are pushing the Court to reanalyze its analog search precedents. In recent years, the Supreme Court has been hesitant to apply its existing Fourth Amendment doctrines to searches of extensive amounts of digital information,[37] reasoning that Fourth Amendment rules like the third-party doctrine were designed for a less-surveilled, pre-digital age and no longer function as intended.[38]

Accordingly, Section I.B will explain how the third-party doctrine was simply not created with the digital age in mind.[39] Today, people engage in transactions with third parties as a necessary part of participating in modern society. These transactions produce digital records of people's daily activities, and, under the third-party doctrine, all of this information is subject to the government's subpoena power. Much of this information was never recorded before the digital age.[40] And even if there was some form of pre-digital record, those records would be much harder for the government to aggregate and analyze, leaving little reason to worry that these records posed major privacy concerns at the time.[41]

A. THE FOURTH AMENDMENT'S REASONABLE EXPECTATION OF PRIVACY TEST

The archetypal Fourth Amendment search involves government officials using arbitrary and general warrants to rummage through homes for

34. *See* Katz v. United States, 389 U.S. 347, 351–53 (1967).

35. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

36. *Id.*

37. For the two recent landmark Supreme Court opinions addressing the application of the Fourth Amendment to digital information, see Carpenter v. United States, 138 S. Ct. 2206, 2214–17 (2018); Riley v. California, 573 U.S. 373, 386 (2014) (requiring a warrant for police officers to search cell phones incident to arrest).

38. *See infra* Section I.B.

39. *See* United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring).

40. *See Carpenter*, 138 S. Ct. at 2218 (discussing how carrying a cell phone is incident to participating in modern society).

41. *See id.* at 2214 (recognizing the "immense storage capacity" of cell phones (citation omitted)).

physical records generally treated as private.[42] Accordingly, it was sufficient for the framers' purposes to safeguard only someone's physical person and property from unreasonable government intrusion in order to protect privacy rights during this era.[43]

The Supreme Court has periodically adjusted its Fourth Amendment jurisprudence in response to new privacy concerns created by improvements in surveillance technology.[44] The seminal case illustrating the Court's shifting understanding of search and seizure law is *Katz v. United States*.[45] *Katz* expanded the reach of the Fourth Amendment to protect people against invasions of their reasonable expectations of privacy, rather than just invasions of their physical persons and property.[46]

Katz dealt with the constitutionality of wiretaps,[47] a surveillance technique that the government did not possess when the Fourth Amendment was drafted. The Supreme Court held that the government's electronic surveillance of a conversation that the petitioner-defendant Charles Katz made within the confines of a public phone booth constituted an unconstitutional search because it violated his reasonable expectation that his communications would be kept private.[48] In doing so, the Court rejected the government's argument that listening electronically to Katz's communications did not constitute a search because it did not physically

42. During colonial times, British officers began using general warrants called "writs of assistance," which gave them arbitrary power to "rummage through homes in . . . unrestrained search[es] for evidence of criminal activit[ies]." *Riley*, 573 U.S. at 403. The colonial opposition to these arbitrary writs "was in fact one of the driving forces behind the Revolution itself." *Id.* (referencing James Otis and John Adams's accounts of the writs of assistance).

43. Moreover, during the time the Bill of Rights was adopted, police officers acted more like night-watchmen than investigators. Wesley MacNeil Oliver, *The Neglected History of Criminal Procedure, 1850–1940*, 62 RUTGERS L. REV. 447, 449–59 (2010). They had little authority—or, for that matter, incentive—to proactively investigate criminal activities. *Id.* As such, there were few concerns that officers would actively seek to invade one's privacy absent prior authorization from a magistrate-issued warrant. *See id.*

Additionally, home-oriented privacy rights dominated the legal scene. The common law axiom that a "man's house is his castle" was "deeply rooted" in United States jurisprudence and "forms part of the fabric of the Fourth Amendment." Jonathan L. Hafetz, *"A Man's Home Is His Castle?": Reflections on the Home, the Family, and Privacy During the Late Nineteenth and Early Twentieth Centuries*, 8 WM. & MARY J. WOMEN & L. 175, 175 (2002) (citations omitted). However, over time, the notion that people's privacy can be protected by simply safeguarding one's home from government intrusion has slowly eroded. *See generally id.* (exploring the application of the constitutional importance of the home to privacy norms developed at the turn of the twentieth century).

44. Kerr, *supra* note 31, at 481–82.

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

46. *See id* at 351.

47. *Id.* at 353.

48. *Id.*

invade the phone booth.[49] The Court held that "the Fourth Amendment protects people, not places," from unreasonable invasions of privacy.[50]

Recognizing the ambiguity of the majority opinion, Justice Harlan's concurrence in *Katz* expounded the reasonable expectation of privacy test, which is the framework applied today.[51] Under this test, courts first ask whether the person had an "actual (subjective) expectation of privacy" and if so, they then determine whether such an expectation is "one that society is prepared to recognize as 'reasonable.' "[52] Justice Harlan explained that Katz was reasonably entitled to "assume" that his communications would be private because the phone booth was completely enclosed when the conversation was made.[53]

After *Katz*, the Supreme Court limited the reasonable expectation of privacy test with the third-party doctrine, which holds that a person does not have a reasonable "expectation of privacy in [the] information he [or she] voluntarily turns over to third parties."[54] In *United States v. Miller*, the Court held that a government subpoena for bank records did not constitute a search because the defendant voluntarily conveyed the information in the records to

49. *Id*. at 352–53.

50. *Id.* at 351. This is somewhat of a misnomer because in its analysis today the Supreme Court determines whether there is a reasonable expectation of privacy based on the place and item that is searched. KERR, *Implementing* Carpenter, *supra* note 11 (manuscript at 5) ("But it was still the place that mattered most in *Katz*, as Justice Harlan's concurrence later adopted by the Court made clear. Justice Harlan dismissed the famous statement that the Fourth Amendment protects people instead of places . . . .").

51. *See* United States v. Jones, 565 U.S. 400, 405–06 (2012) (citing *Katz*, 389 U.S. at 360 (Harlan, J., concurring)).

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

53. *Id.* (citation omitted). The problem with this test is that it forces courts to engage in a circular analysis. *See Jones*, 565 U.S. at 427–28 (Alito, J., concurring in the judgment) ("[*Katz*] involves a degree of circularity, and judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks. In addition, the *Katz* test rests on the assumption that [the] hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations." (citations omitted)).

54. Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (citing United States v. Miller, 425 U.S. 435, 442–44 (1976)). For further discussion on the third-party doctrine, see Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009); Solove, *supra* note 7, at 526–27. Another similar limitation to *Katz* is aptly articulated by the facts of *United States v. Knotts,* 460 U.S. 276, 281 (1983), which holds that a person driving their car on public roadways "has no reasonable expectation of privacy in his [or her] movements from one place to another." The Court reasoned that the government's use of a beeper that emitted a radio signal, telling authorities where the defendant was travelling, was not a Fourth Amendment search because the defendant "voluntarily conveyed" his travels to the other drivers on the roadway. *Id*. at 281–82. Thus, the information uncovered by the beeper on the defendant's car would be equivalent to information the police would have uncovered from visually surveilling the defendant throughout the course of the day. *Id.* at 282. This doctrine has been since limited by the Court in *United States v. Jones*, 565 U.S. 400, 404–11 (2012).

the bank, making his expectation that the information would be kept private unreasonable.[55] Three years later in *Smith v. Maryland*, the Court likewise held that the government's electronic recording of phone numbers that a defendant dialed onto his phone did not constitute a search because he conveyed the numbers to the phone company in order to route his call.[56] As such, the defendant's expectation that the numbers he dialed would be kept private was unreasonable.[57]

The third-party doctrine has two crucial features. First, it only gives the government access to non-content information, which theoretically is less invasive than content information.[58] In *Smith*, for example, the government only accessed the phone numbers that the defendant dialed and did not listen in on the actual *content* of the conversations.[59] Second, it rests on the categorical presumption that if information is voluntarily conveyed to third parties, it is not secret, and therefore does not warrant Fourth Amendment protection; essentially, if someone chooses to share information with another, they cannot expect it to be private.

B. THE THIRD-PARTY DOCTRINE IN THE DIGITAL AGE

At the time *Miller* and *Smith* were decided, the third-party doctrine functioned as a reasonable privacy tradeoff. It created a bright-line rule that allowed courts and government officials to easily distinguish between the types of information that required a warrant and the types that did not, while still allowing a substantial sphere of space in which people could exclude the government. This sphere of privacy, however, has significantly eroded in the digital age due to the increasing invasiveness of aggregated non-content information and the lack of choice people have in sharing such information with third parties.[60]

55. United States v. Miller, 425 U.S. 435, 440–41 (1976).

56. *Smith*, 442 U.S. at 741–44. For an argument that the justices in *Smith* may have intended the decision to be narrower than it turned out to be, see Neil Richards, *The Third-Party Doctrine and the Future of the Cloud*, 94 WASH. U. L. REV. 1441, 1472–74 (2017).

57. *Smith*, 442 U.S. at 741–44.

58. For further discussion on *Carpenter* and the difference in constitutional protections for content and non-content information, see KERR, *Implementing* Carpenter, *supra* note 11 (manuscript at 1–20).

59. *Smith*, 442 U.S. at 741.

60. *See* SOLOVE, *supra* note 4, at 165–68. Justice Marshall dissented in *Smith* because the third-party doctrine rests on the rather categorical presumption that information is either wholly private, and thus protected by the Fourth Amendment, or not. *Smith*, 442 U.S. at 749 (Marshall, J., dissenting). Justice Marshall explained that "[p]rivacy is not a discrete commodity, possessed absolutely or not at all." *Id.* He believed the third-party doctrine's assumptions that people's privacy rights can be rationalized in a categorical rule were erroneous. *Id.* The digital age highlights the salience of Justice Marshall's dissent. Justice Sotomayor, relying on Justice Marshall's dissent in *Smith*, recently criticized the third-party doctrine as "ill suited to the digital age." United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor,

In the aggregate, non-content information can be extremely revealing—to the point where it can depict the *contents* of someone's life.[61] For example, each discrete piece of non-content CSLI gathered by the government is relatively non-invasive because it only tells the government where the suspect was at a given point in time. It does not tell the government about the content of the suspect's activities at that instance in time. However, several days' worth of CSLI put together can reveal intimate information about a suspect's life, such as his or her routine, habits, friends, and so forth.[62] In the past, this was less concerning because if the government wanted to track a suspect's movements with relative precision, it needed to expend considerable resources to physically follow the suspect around all day. But in the digital age, before the *Carpenter* decision was handed down, this information was accessible through a third-party subpoena request.[63]

Moreover, sharing information with third parties has become a necessity of participating in modern society. The third-party doctrine presumes that information is conveyed to third-parties "voluntarily," which made sense at the time *Miller* and *Smith* were decided.[64] *Smith*, for example, discussed how it was unreasonable for the defendant to think that the telephone numbers he dialed would be private because dialing a number on a telephone was not materially distinguishable from verbally telling an operator the person he wanted to call.[65] Today, however, people have no choice but to share personal information with third-party intermediaries as a part of daily life, and it is therefore unreasonable that the law does not recognize that people can have privacy rights in information shared with

J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."). Justice Sotomayor argued that digital information disclosed only for limited purposes should not automatically be "disentitled to Fourth Amendment protection." *Id.* at 418.

61. *See* Rosenzweig, *supra* note 23 ("The fundamental idea [behind the mosaic theory] is that aggregations of data create information beyond their individual value. 1+1+1 equals 17, not just 3."). It may be argued that the third-party doctrine's reasoning is still sound in the digital age, but that its binary application may no longer apply. Prior to the digital age, there was virtually no chance that someone's privacy would be invaded from the government's access to non-content information because it was so hard to aggregate. Now, each discrete piece of third-party metadata is actually fractionally invasive, and the invasiveness of each piece of data grows exponentially depending on how much has already been gathered. Thus, when the government compiles substantial sums of metadata, it can be constitutionally invasive. *See id.*

62. Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018); Rosenzweig, *supra* note 23.

63. *See Carpenter*, 138 S. Ct. at 2213, 2217 (reversing the lower court opinion that held no Fourth Amendment search occurred when the government accessed 127 days of CSLI).

64. *See id*.

65. Smith v. Maryland, 442 U.S. 735, 744–45 (1979).

these parties for limited purposes.[66] Although people may think that the convenience they receive from providing third parties with their digital information makes the tradeoff "worthwhile" or even "inevitable,"[67] this concept of voluntariness embedded in the third-party doctrine does not adequately track contemporary privacy norms.[68]

II. THE *CARPENTER* SHIFT

Chief Justice Roberts's landmark opinion in *Carpenter v. United States* was lauded by many for refusing to apply the third-party doctrine.[69] The problem is, however, that *Carpenter* does not leave much law for practitioners and lower courts to work with.[70] It merely flags the narrow issue that broad requests for CSLI will require a warrant while punting the job of articulating clear digital search rules down the road for another day.[71]

Carpenter is ambiguous on two separate axes.[72] The first notable ambiguity is that the Court did not outline a criterion under which lower courts could determine whether and how *Carpenter* extends to cases dealing with different types of digital information.[73] This Note, however, focuses on *Carpenter*'s second key ambiguity—that the Court did not tell lower courts how to determine when the government's access to these digital records constitutes a Fourth Amendment search.[74] One method that has been proposed to determine when a search occurs is the source rule, which holds

66. *See* Daniel Solove, *10 Reasons Why the Fourth Amendment 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/9NLX-MKGJ].

67. United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring in the judgment).

68. *Id.* at 417–18 (Sotomayor, J., concurring) ("I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year.").

69. *See, e.g.*, Mark Joseph Stern, *A Historic Victory for Privacy*, SLATE (June 22, 2018, 11:41 AM), https://slate.com/news-and-politics/2018/06/carpenter-v-united-states-supreme-court-rules-fourth-amendment-protects-cell-phone-location-records-in-an-opinion-by-chief-justice-john-roberts.html [https://perma.cc/XHZ4-DXDC] ("*Carpenter* is an earthquake in Fourth Amendment law, modernizing the right to privacy for what [Justice] Kennedy calls 'the Cyber Age.' No longer will the court pretend that CSLI is indistinguishable from telephone numbers and bank records.").

70. *See* Rosenzweig, *supra* note 17 ("[T]he Supreme Court's decision in *Carpenter v. United States* is not law. Anyone who says they can read the majority opinion and predict with any degree of confidence how the Court will deal with any number of future technologies—be they biometrics, facial recognition, DNA or real-time [CSLI]—is, frankly, just making it up.").

71. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) ("Our decision today is a narrow one. We do not express a view on matters not before us . . . .").

72. Kerr has devoted two chapters in his forthcoming book on this topic—one for each axis; for these two chapters, see generally KERR, *Implementing* Carpenter, *supra* note 11.

73. *Id.* (manuscript at 2–3).

74. *Id.* (manuscript at 27).

that "[i]f the government learned any fact sourced from any *Carpenter*-covered [digital] record, then that information transfer is a search," regardless of how much digital information was obtained.[75] Another method is the mosaic theory, which asks whether the *quantity* of digital records accessed by the government violates people's reasonable expectations of privacy.[76]

Section II.A will more thoroughly introduce the facts of *Carpenter* and explain how it did not adequately define how to determine when a search of CSLI-like information occurs. Then, Section II.B will discuss the mosaic theory in more detail through a discussion of *United States v. Jones*.[77] It will then weigh the virtues of the source rule and the mosaic theory as possible tests to determine when a *Carpenter* search occurs.

A. *CARPENTER V. UNITED STATES* AND ITS LACK OF CLARITY

In *Carpenter*, the Court dealt with the profoundly invasive implications that its analog-search precedents have created in the digital age.[78] The petitioner-defendant, Timothy Carpenter, was convicted of robbing a series of Radio Shack and T-Mobile stores in Detroit with help from various accomplices.[79] In the course of the FBI's investigation into Carpenter and his co-conspirators, the FBI subpoenaed 127 days' worth of CSLI from their wireless carriers.[80] The CSLI allowed the government to determine the suspects' general locations based on what cell tower their phones were connected to at various times of the day.[81] This information was used to convict Carpenter at trial by showing that his phone was near several of the robberies while they occurred.[82] The Sixth Circuit affirmed the conviction on the grounds that the CSLI was admissible under the third-party doctrine because Carpenter voluntarily conveyed his location to the cell phone carriers to establish a means for communication.[83]

Chief Justice Roberts's majority decision in *Carpenter*, joined by

75. *Id.* (manuscript at 28).

76. *Id.* (manuscript at 27–28).

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

78. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("[W]e hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI.").

79. *Id.* at 2212.

80. *Id.*

81. *Id.* at 2211–12. "Altogether the Government obtained 12,898 location points cataloging Carpenter's movements—an average of 101 data points per day." *Id.* at 2212.

82. *Id.* at 2213.

83. *See id.*

Justices Breyer, Ginsburg, Kagan, and Sotomayor, reversed Carpenter's conviction, holding that the government's acquisition of 127 days' worth of CSLI violated his reasonable expectation of privacy in the whole of his physical movements.[84] Essentially, the Court held the third-party doctrine did not apply because *Smith* and *Miller* could not have contemplated the extremely invasive nature of CSLI and the ease at which the government could obtain it.[85] In doing so, the Court explained that advances in information technology pose serious threats to Fourth Amendment privacy protections and the third-party doctrine.[86] It further reasoned that this outcome was necessary to restrict the police from engaging in "too permeating police surveillance" and to protect the "privacies of life."[87]

Despite its strong inclination to stand in the way of a government with "near perfect surveillance"[88] capabilities, the *Carpenter* Court left practitioners and lower courts with very little precedential guidance. Admittedly, this was probably by design. Quoting Justice Frankfurter, the Chief Justice explained that "the Court must tread carefully" before adopting legal frameworks to address technological innovations "to ensure that [it does] not 'embarrass the future.' "[89] *Carpenter* was thus intentionally "narrow" and did not "call into question conventional surveillance techniques and tools."[90] Instead, it merely represents the "rare" occasion when the third-party doctrine does not apply.[91]

Along this cautious vein, Chief Justice Roberts explained in a footnote that it was "sufficient for [the Court's] purposes . . . to hold that accessing

84. *Id.* at 2211, 2223.

85. *Id.* at 2220 ("We therefore decline to extend *Smith* and *Miller* to the collection of CSLI. Given the unique nature of cell phone location information, the fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection.").

86. *Id.* at 2222 ("CSLI is an entirely different species of business record—something that implicates basic Fourth Amendment concerns about arbitrary government power much more directly than corporate tax or payroll ledgers.").

87. *Id.* at 2214 (citations omitted). In its ruling, the Court incorporated pieces of the arguments from each of the concurring opinions advocating for the mosaic theory in *Jones*. Thus, the Court did not give a clear indication of what it considers the driving policy mechanism behind mosaic searches. *Id.* at 2220.

88. *Id.* at 2218.

89. *Id.* at 2220 (quoting Nw. Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944)); *see also* Nina Totenberg, *In Major Privacy Win, Supreme Court Rules Police Need Warrant To Track Your Cellphone*, NPR: ALL THINGS CONSIDERED (June 22, 2018, 10:41 AM), https://www.npr.org/2018/06/22/605007387/supreme-court-rules-police-need-warrant-to-get-location-information-from-cell-to [https://perma.cc/4B3X-S4XR] ("Justice Breyer, who joined [the *Carpenter*] majority opinion, may have foreseen some of these problems at oral argument. 'This is an open box,' he said. 'We know not where we go.' ").

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

91. *Id.* at 2222.

seven days of CSLI constitutes a Fourth Amendment search."[92] Overall, this limited holding at least suggests that *Carpenter* created a seven-day ceiling on the amount of information that the government may request from third parties without a warrant.[93] What remains unclear is what the Court plans to do with this ceiling as technology and jurisprudence in this area develop.

B. THE CHOICE BETWEEN THE SOURCE RULE AND THE MOSAIC THEORY[94]

The Supreme Court is left with a few options as to how to determine when a *Carpenter* search occurs. Although *Carpenter* seemed most concerned with the alarming quantity of information the government was able to acquire, its holding does not preclude the Court from eventually following the source rule,[95] which would require the government to get a warrant to access *any* digital information similar to CSLI.[96] The source rule looks at the quality of the information that is gathered by the government, rather than the quantity of information that it accumulates.[97]

Alternatively, *Carpenter* could be read to endorse the mosaic theory. The mosaic theory takes a more holistic approach by looking at police activity as a collective whole to determine whether a Fourth Amendment search has occurred, even if each step along the way did not constitute a search.[98] In arriving at its conclusion in *Carpenter*, the Court relied heavily on the respective concurring opinions of Justices Alito and Sotomayor in *United States v. Jones*.[99] These concurring opinions, which were supported by the combined votes of five Justices, stood for the notion that the Court is concerned more with long-term rather than short-term digital surveillance.[100]

92. *Id.* at 2217 n.3. It is important to note that the Court reserved holding whether any government requests for third parties to turn over CSLI or other like information would constitute a Fourth Amendment search. *Id.* The Court is certainly within its power to simply state in the future that the third-party doctrine does not apply; however, this would be a drastic scenario given the abundance of instances in which the third-party doctrine adequately addresses privacy norms. *See generally* Kerr, *supra* note 54 (defending the third-party doctrine's application and reasoning in most scenarios).

93. Kerr has described this to be a "cap" on the existing Fourth Amendment doctrine. Kerr, *supra* note 15.

94. Kerr also suggests a third alternative, the "Subjective Approach," which focuses on "when the government learned the kind of private information that *Carpenter* safeguards." KERR, *Implementing* Carpenter, *supra* note 11 (manuscript at 27). This would require a case-by-case analysis on what the government already knows about a particular suspect being surveilled in order to determine when a search occurs, whereas the mosaic approach is more objective. *Id.* (manuscript at 28–29). Because of the myriad of flaws that the subjective approach has, this Note will not discuss it further.

95. *See Carpenter*, 138 S. Ct. at 2217 n.3.

96. KERR, *Implementing* Carpenter, *supra* note 11 (manuscript at 27–28).

97. *Id.* (manuscript at 28).

98. Kerr, *supra* note 21, at 313–14.

99. *See Carpenter*, 138 S. Ct. at 2215 (citations omitted).

100. Kerr, *supra* note 21, at 313.

Moreover, at least one state court of last resort has read *Carpenter* to allow the government to access CSLI in smaller batches without a warrant.[101]

Section II.B.1 will first outline the Supreme Court's understanding of the mosaic theory through a discussion of *Jones*.[102] Then, Section II.B.2 will compare the merits of the source rule and the mosaic theory, ultimately arriving at the conclusion that the mosaic theory is more theoretically sound but would be much more difficult to administer.

1. The Mosaic Theory as Explained in *United States v. Jones*

The mosaic theory diverges substantially from the "sequential approach" that courts currently employ to determine when a search occurs on a given set of facts.[103] Under the sequential approach, courts ask whether each government action over the course of an investigation—no matter how innocuous the action may have been—invaded a defendant's reasonable expectation of privacy.[104] Consider the following illustrations:

> If an officer inserts a key into the door of a residence and then opens the door to enter, a reviewing court will first consider the act of inserting the key and then analyze the distinct act of opening the door. If an officer sees expensive stereo equipment in an apartment, moves it to see the serial number, and then records the serial number, a court will treat moving the equipment as distinct from recording the number. If an officer sees suspects preparing for a robbery, stops them, and pats them down for weapons, the court will consider the viewing, the stopping, and the patting down as distinct acts that must be analyzed separately.[105]

Alternatively, the mosaic theory rests on the idea that, in the aggregate, even normally non-invasive information—for example, digital metadata—can invade one's reasonable expectations of privacy.[106] This concept is fairly intuitive; the invasiveness of any given piece of information depends on what other information is known at the time. As such, the mosaic theory necessarily takes a more holistic approach to determine when a Fourth Amendment search materializes.

101. Sims v. State, 569 S.W.3d 634, 645–46 (Tex. Crim. App. 2019) ("Whether a particular government action constitutes a 'search' or 'seizure' . . . turns on whether the government searched or seized 'enough' information that it violated a legitimate expectation of privacy. . . . Here, Appellant did not have a legitimate expectation of privacy . . . in the less than three hours of real-time CSLI records accessed by police . . . .").

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

103. Kerr, *supra* note 21, at 315–16.

104. *Id*.

105. *Id.* at 316 (footnotes omitted).

106. KERR, *Implementing* Carpenter, *supra* note 11 (manuscript at 35–36).

The underpinnings of the mosaic theory are perhaps best articulated through a discussion of the various judicial opinions surrounding *United States v. Jones*.[107] *Jones* dealt with whether the government's installation of a GPS tracking device on defendant Antoine Jones's car to monitor his movements over the course of twenty-eight days constituted a Fourth Amendment search.[108] Jones was a nightclub owner whom the FBI suspected was trafficking narcotics.[109] In the course of their investigation, and without a valid warrant, FBI agents installed a GPS device on Jones's car and tracked his movements for twenty-eight days.[110] The GPS data proved "essential" to the government's conspiracy case, as it allowed the prosecutors to "paint a picture of Jones's movements" to show that he was involved in the trafficking.[111] At trial, the GPS evidence was admitted because Jones voluntarily conveyed his location to other people on the roadways by driving on public streets.[112] Jones was found guilty of drug conspiracy charges.[113]

On appeal, Judge Douglas H. Ginsburg of the D.C. Circuit reversed the conviction, holding that the installation and long-term monitoring of the GPS device was a Fourth Amendment search.[114] Judge Ginsburg conceded that Jones did not have a reasonable expectation of privacy in each individual trip he made in his car because each was exposed to the public.[115] Nonetheless, Judge Ginsburg reasoned that Jones had a reasonable expectation of privacy in the totality of his movements because the "likelihood anyone [would have] observe[d] all those movements [was] effectively nil."[116]

The Supreme Court affirmed the ruling, but on different grounds—

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

108. *Id.* at 402–03.

109. *Id*. at 402.

110. *Id.* at 403 & n.1. In *Jones*, the government did have a warrant to install the GPS device, but the government's installation of the GPS device was not within the scope of the warrant because the government agents did not comply with its instalment requirements. *Id*. Accordingly, the government argued that no warrant was needed because the installation of the device was not a "search" within the meaning of the Fourth Amendment. *Id.*

111. United States v. Maynard, 615 F.3d 544, 567 (D.C. Cir. 2010), *aff'd in part sub nom*. United States v. Jones, 565 U.S. 400 (2012).

112. *Jones*, 565 U.S. at 403–04. Therefore, he had no reasonable expectation of privacy in this information and the government accessing it did not constitute a Fourth Amendment search. *Id.* (citing United States v. Knotts, 460 U.S. 276, 281 (1983)).

113. *Id.* at 404.

114. *Maynard*, 615 F.3d at 563–66.

115. *Id.*

116. *Id.* at 558.

setting the mosaic theory aside for another day.[117] Justice Scalia's majority opinion held that the physical installation of the GPS system on Jones's car constituted a search because it involved the government's physical "trespass" onto Jones's property.[118] As a result, the most interesting part of *Jones* is found in the concurrences from Justices Alito and Sotomayor, respectively. Read together, these concurrences garner five votes in favor of deciding the case on mosaic grounds.[119]

Justice Sotomayor's version of the mosaic theory argued that Jones's reasonable expectation of privacy was violated because people do not "reasonably expect that their movements will be recorded and aggregated in a manner that enables the [g]overnment to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[120] Justice Sotomayor seemed concerned that the government's unfettered ability to use GPS monitoring would "chill[] associational and expressive freedoms."[121]

Justice Alito's concurrence, joined by Justices Breyer, Ginsburg, and Kagan, grounded its argument for the mosaic theory on the distinction between short-term and long-term surveillance.[122] Put simply, a search occurs because people do not think that the government will "secretly monitor and catalogue" someone's movements in the long-term.[123] Justice Alito added that this expectation was reasonable because, historically, law enforcement officials needed to expend a considerable amount of resources to surveil a suspect in the long-term, making such surveillance practically infeasible in most cases.[124]

In sum, *Jones* provides three judicial opinions attempting to justify the need for the mosaic theory. Judge Ginsburg argued that even if each of Jones's discrete movements were exposed to the public, the collective

117. *Jones*, 565 U.S. at 412–13 ("It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.").

118. *Id.* at 404–05.

119. Carpenter v. United States, 138 S. Ct. 2206, 2215 (2018) (counting five votes in favor of the mosaic theory from *Jones*).

120. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

121. *Id*. This rationale is reminiscent of the subjective approach that Kerr explained was a possible, yet flawed, option that the Court could use to determine when a *Carpenter* search occurs. KERR, *Implementing* Carpenter, *supra* note 11 (manuscript at 28) ("If access to records counts as a search because it paints an intimate portrait of a person's life, why not say a search occurs when the portrait has been painted? Just watch what the government knows. When it learns something invasive, a search has occurred.").

122. *See Jones*, 565 U.S. at 430–31 (Alito, J., concurring in the judgment).

123. *Id.* at 430.

124. *Id.*

amount of information that the government gathered was not exposed.[125] Essentially, his argument is that the aggregate of the location information is more invasive than each discrete datum.[126] Justice Sotomayor seemed most concerned with the notion that the precision and expansiveness of GPS surveillance can potentially chill behavior.[127] Justice Alito, on the other hand, argued that people have a reasonable expectation that the government is not going to track their movements over the course of several days.[128]

2. Comparing the Source Rule and the Mosaic Theory

At bottom, the choice between the source rule and the mosaic theory comes down to whether courts want a rule that is simpler to apply or one that better reflects the reality of digital privacy invasions.[129] Under the source rule, all government investigators would have to know before gathering information on a suspect is whether the information they want to gather is digital and subject to *Carpenter*.[130] If *Carpenter* does control, the government would need a warrant to access the information, and vice versa. This analysis fits squarely within the sequential approach that courts are familiar with. Additionally, the source rule leads to the simpler application of the exclusionary rule: if the government accesses this information without a warrant, and no exception to the exclusionary rule applies, all the digital information gathered would be excluded from use at trial.

This simplicity comes at a price; the source rule is over-inclusive whereas the mosaic theory better tethers the warrant requirement to real privacy invasions.[131] The government's acquisition of digital metadata only invades a suspect's reasonable expectation of privacy in this information when the government gets a sufficient quantity of it.[132] Therefore, the source rule would prohibit the government from accessing a lot of relevant digital information in ways that are constitutionally non-invasive without a warrant. For example, a recent Texas Court of Criminal Appeals case applying *Carpenter* held that the police's access to less than three hours of CSLI records did not invade a defendant's reasonable expectation of privacy.[133]

125. *See* United States v. Maynard, 615 F.3d 544, 563–66 (D.C. Cir. 2010).

126. *See id*.

127. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

128. *Id.* at 430–31 (Alito, J., concurring in the judgment).

129. KERR, *Implementing* Carpenter, *supra* note 11 (manuscript at 28).

130. *See id.*

131. *Id.* (manuscript at 27–28).

132. *See Jones*, 565 U.S. at 416 (Sotomayor, J., concurring); *id.* at 430 (Alito, J., concurring in the judgment); United States v. Maynard, 615 F.3d 544, 563–66 (D.C. Cir. 2010).

133. Sims v. State, 569 S.W.3d 634, 645–46 (Tex. Crim. App. 2019). The Texas Court of Criminal Appeals is Texas's highest criminal court.

Under the source rule, the Texas police's access to these three hours of CSLI—which is likely not enough for the police to be able to paint a picture of the defendant's behaviors—would require a warrant.

On the other hand, for the mosaic theory to closely track the invasiveness of aggregated digital information, courts would have to engage in an extensive amount of line-drawing. *Carpenter* provided one durational limitation—that the government needed a warrant to access seven or more days of CSLI[134]—but this limitation is easily distinguishable. Moreover, *Carpenter*'s seven-day ceiling will likely be tightened because it was artificial; seven days was simply the smallest quantity of CSLI information that was requested in one subpoena.[135] At oral argument Carpenter's own attorney suggested that the Court adopt a rule that would allow the government to access no more than twenty-four hours of CSLI without a warrant.[136] It is therefore not unreasonable to conclude that the Court could seek to lower the mosaic threshold for CSLI requests as it gets a better grasp on digital privacy norms or if a closer case presents itself.

Additionally, courts would be required to periodically redraw many of these durational limits as technology improves.[137] Justice Kennedy, in his dissent in *Carpenter*, pointed out that CSLI is actually fairly imprecise.[138] Thus, if *Carpenter* holds that seven days of this relatively imprecise CSLI is enough to violate one's reasonable expectation of privacy, it is safe to imagine that as CSLI technology becomes more precise, a mosaic search could occur when the government acquires a smaller quantity of it. This is problematic because courts may not have the bandwidth to adapt their durational limitations quickly enough to keep up with inevitable advances in surveillance technology.

Although the Supreme Court has been reluctant to create bright-line durational limits in its criminal procedure jurisprudence, it has done so when

134. Carpenter v. United States, 138 S. Ct. 2206, 2217 n.3 (2018).

135. *See id.*; Bellovin et al., *supra* note 22, at 625 ("Tracking the location of a person for even just a few days may be enough to reveal a lot of protected information."). Moreover, footnote three in *Carpenter* only limits the amount of CSLI "accessed" by the government. *See Carpenter*, 138 S. Ct. at 2217 n.3. Therefore, the Court left open whether a search would occur when the government requests over seven days of CSLI, but only actually gets access to a few days of data.

136. Transcript of Oral Argument at 9, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402).

137. *See* Kerr, *supra* note 21, at 347 ("[T]he constantly evolving nature of surveillance practices can lead new questions to arise faster than courts might settle them. Old practices would likely be obsolete by the time the courts resolved how to address them, and the newest surveillance practices would arrive and their legality would be unknown.").

138. *Carpenter*, 138 S. Ct. at 2225 (Kennedy, J., dissenting).

necessary.[139] In *County of Riverside v. McLaughlin*,[140] the Court dealt with an ambiguity in criminal procedure it left in *Gerstein v. Pugh*,[141] which "held that the Fourth Amendment requires a prompt judicial determination of probable cause . . . following a warrantless arrest."[142] The Court in *McLaughlin* therefore had to determine what constituted a "prompt" probable cause hearing.[143] In doing so, the Court announced that, "as a general matter," a probable cause hearing administered "within 48 hours of arrest will . . . comply with the promptness requirement," barring exceptional circumstances.[144]

It is at least plausible that the Court in future cases would similarly articulate reasonable durational limits for the mosaic theory.[145] In *McLaughlin*, the Court created this durational guideline "to provide some degree of certainty so that [government officials] may establish procedures with confidence that they fall within constitutional bounds."[146] Likewise, the mosaic theory certainly has the potential to create substantial confusion on the part of legislatures and law enforcement officers as to when their investigatory techniques require a warrant.[147]

III. APPLYING THE EXCLUSIONARY RULE TO MOSAIC SEARCHES

The mosaic theory does not fit neatly into the Court's existing Fourth Amendment search doctrine.[148] Even if courts were to create robust durational limits to tell government agents what quantity of information they can access constitutionally, implementing the mosaic theory would still

139. Orin Kerr, *Four Thoughts on the Briefing in* Carpenter v. United States, LAWFARE (Nov. 17, 2017, 3:06 PM), https://www.lawfareblog.com/four-thoughts-briefing-carpenter-v-united-states [https://perma.cc/NAU9-KVSV]. The fact that the Court in *Carpenter* did not provide a bright-line boundary, even though it did say that at least seven days of CSLI was enough to require a warrant, exemplifies this notion. *See Carpenter*, 138 S. Ct. at 2217 n.3.

140. Cty. of Riverside v. McLaughlin, 500 U.S. 44 (1991).

141. Gerstein v. Pugh, 420 U.S. 103 (1975).

142. *McLaughlin*, 420 U.S. at 47.

143. *Id.*

144. *Id.* at 45, 56.

145. This is especially the case given that this Court has been recently willing to evade or even overrule precedent in order to protect people's digital privacy. *See* Carpenter v. United States, 138 S. Ct. 2206, 2215–20 (2018); Riley v. California, 573 U.S. 373, 401–03 (2014).

146. *McLaughlin*, 420 U.S. at 56.

147. Kerr, *supra* note 21, at 341 ("If courts cannot specify ex ante with clarity when police conduct aggregates sufficiently to constitute a search, officers may understandably cross the line without personal culpability."). *But see* Kerr, *supra* note 139 (expressing doubt that this line of reasoning is a winning one).

148. Kerr, *supra* note 21, at 314–15.

require answering a mess of additional doctrinal questions.[149] One of these questions, and perhaps the most salient one, deals with how to apply the exclusionary rule to mosaic search violations.[150] The exclusionary rule is the primary remedy for Fourth Amendment violations and allows criminal defendants to seek to suppress unconstitutionally obtained evidence at trial.[151]

In order to determine how to best apply the exclusionary rule to mosaic searches, the following questions must be answered: (1) How *could* the exclusionary rule apply? (2) And how *should* the exclusionary rule apply? Section III.A will introduce the exclusionary rule. Section III.B articulates two readily apparent approaches that courts could utilize to apply the exclusionary rule to mosaic searches but ultimately explains that these approaches are flawed. The first approach, the "all-or-nothing approach," holds that all evidence derived from a mosaic search should be excluded, regardless of when the search actually occurred. The second approach, the "after-search approach," excludes only the evidence in a mosaic search that was gathered after the mosaic threshold was crossed. Finally, Section III.C proposes a middle-ground approach, the "after-act approach," which excludes all the evidence from the single government act that triggered the mosaic search, and any subsequent act thereafter. This approach is meant to reconcile the flaws of the all-or-nothing and after-search approaches and provide a plausible answer to the mosaic theory's exclusionary problem.

A. THE EXCLUSIONARY RULE

The exclusionary rule provides defendants with a remedy for violations of their Fourth Amendment rights to be secure against unreasonable searches and seizures.[152] Accordingly, evidence obtained in violation of the Fourth Amendment is generally inadmissible in the criminal trial of the person whose rights were violated.[153]

The exclusionary rule is prophylactic and one of judicial advent. The Fourth Amendment does not expressly provide a remedy for violations of its provisions.[154] Essentially, without the exclusionary rule, the government

149. *Id.*

150. *Id.* at 340–43.

151. *Id.* at 340.

152. Hudson v. Michigan, 547 U.S. 586, 590 (2006).

153. *Id.* For a comprehensive historical account and criticism of the exclusionary rule, see Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 785–800 (1994).

154. United States v. Leon, 468 U.S. 897, 906 (1984) (citing United States v. Calandra, 414 U.S. 338, 348 (1974)).

would be incentivized to violate people's Fourth Amendment rights, unacceptably reducing the Constitution to a "form of words."[155]

One cannot properly discuss how to fashion an approach to applying the exclusionary rule without first recognizing that judges do not apply the rule with enthusiasm; instead judges only exclude evidence as a "last resort."[156] The exclusionary rule primarily protects criminal defendants who are guilty. Thus, its application generates "substantial social costs" by "setting the guilty free."[157] As such, the Court has limited the exclusionary rule by articulating exceptions calculated to help balance the rule's benefits and costs and applying it only when necessary to deter future constitutional violations.[158] In fact, it is often easier as a defendant to prove that the Fourth Amendment was violated than to receive a remedy for its violation.

155. *Mapp*, 367 U.S. at 648 (quoting Silverthorne Lumber Co. v. United States, 251 U.S. 385, 392 (1920) (Holmes, J.)). A prime example of the importance of the deterrent effect of the exclusionary rule is found in *United States v. Payner*, 447 U.S. 727, 730–31, 736–37 (1980). In *Payner*, the police "knowingly and willfully" engaged in an unlawful seizure of the defendant's banker's records, *id.* at 730 (citation omitted), presumably because the officers knew that the true defendant would not have standing to use the exclusionary rule to suppress the evidence uncovered, *id.* at 734–37. This Fourth Amendment violation led to the discovery of evidence that was used to convict the defendant at trial. *Id*. at 733–37. The Sixth Circuit held that the evidence was inadmissible under the supervisory power, *id.* at 731, but the Supreme Court reversed, strictly applying the standing requirement, and thus condoning the officers' intentional violation of the banker's rights, *see id.* at 735–37.

156. *Hudson*, 547 U.S. at 591.

157. *Id.* (citation omitted).

158. Under the good-faith exception to the exclusionary rule, if government officers conducting a search have an objectively reasonable, good-faith belief that they were acting lawfully, evidence found pursuant to the search would be admissible at trial. Davis v. United States, 564 U.S. 229, 238–40 (2011). The reasoning behind this exception is that the marginal deterrence effect provided from holding the government strictly liable for constitutional violations is outweighed by the substantial costs of excluding relevant evidence of guilt. *Id.* Accordingly, the good-faith exception allows the admission of the fruits of an unconstitutional search conducted in reliance on clearly established appellate precedent authorizing such a search, and only later find that such precedent was invalid. *See generally id.*

Additionally, even if the good-faith exception does not apply, the exclusionary rule still may not apply if the need for deterrence is too attenuated from the interests protected by the constitutional rule that was violated. In *Hudson v. Michigan*, 547 U.S. 586, 588–90 (2006), the Supreme Court dealt with whether a law enforcement official's "violation of the 'knock-and-announce' rule require[d] the suppression of all evidence found in [a subsequent] search." In *Hudson*, the government officers who searched the defendant's house pursuant to a valid warrant did not wait a reasonable time before entering the defendant's residence and found large quantities of drugs while inside. *Id.* at 588. The Supreme Court held the exclusionary rule did not apply, *id.* at 599, reasoning that the interests protected by the exclusionary rule, deterring arbitrary and unreasonable government searches, were too attenuated from the interests protected by the knock-and-announce rule, the protection of life, property, and "dignity that can be destroyed by a sudden entrance," *id.* at 594, 599.

B. HOW COULD THE EXCLUSIONARY RULE APPLY?

There are two approaches to applying the exclusionary rule to mosaic searches that are immediately apparent: exclude all the digital evidence gathered from the search or exclude only the evidence gathered after the mosaic threshold was crossed.[159] These two approaches, which this Note will refer to as the all-or-nothing and after-search approaches, respectively, are problematic. In summary, the all-or-nothing approach is overly harsh on government officers and will cause a lot of evidence to be lost whereas the after-search approach does not really deter government officers from making broad requests for digital information.

1. The "All-Or-Nothing" Approach

The all-or-nothing approach requires the exclusion of all evidence the government acquired by way of a mosaic search, regardless of when exactly the mosaic search occurred. Imposing an all-or-nothing standard in favor of exclusion would seriously deter government agents from engaging in broad acquisitions of digital information without first getting a warrant. Additionally, the all-or-nothing approach is much simpler to apply once a mosaic search violation is identified. On the other hand, this approach will

159. Perhaps before explaining how the exclusionary rule could apply to evidence found in an unconstitutional mosaic search, this Note should first assess whether the exclusionary rule applies at all. For example, a hard question is whether the good-faith exception would apply to evidence obtained by the police in an unconstitutional mosaic search when the mosaic threshold was not clearly established. Such a situation would likely occur frequently due to the constant line-drawing that the mosaic theory would require. There will invariably be divergences between the rapid speed with which digital surveillance technology develops and the slow pace with which the judiciary responds to these advancements. A thorough analysis on this topic would require further discussion beyond the scope of this Note.

Thus, this Note will assume that the good-faith exception will not apply when police act in the absence of clearly established precedent allowing such actions. After all, thus far, the Court has cabined the good-faith exception to cases in which the government acted reasonably in reliance on some law or information affirmatively authorizing them to conduct the search that was later deemed unconstitutional. One could imagine, however, a standard that holds the good-faith exception to continue to apply when the police act in an objectively reasonable manner in the face of ambiguous legal standards. If this were the case, then the source rule should be preferred over the mosaic theory.

Kerr has also argued that the exclusionary rule may not apply to mosaic searches under *Hudson* because mosaic searches could be "plausibly analogize[d]" to violations of the knock-and-announce rule because "[b]oth involve murky standards and would likely draw significant litigation." Kerr, *supra* note 21, at 340–41. This argument overextends *Hudson*. Courts should not altogether avoid using the exclusionary rule in conjunction with the mosaic theory because it would be difficult. Moreover, unlike in *Hudson*, in which the privacy interests protected by the knock-and-announce rule were secondary and minimal, *Hudson*, 547 U.S. at 594, mosaic searches present profound privacy concerns. Justice Sotomayor explained the impact of these privacy considerations in *Jones*, basing her mosaic analysis on the protection of individual rights—namely, free speech and freedom of association. *See* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

over-deter digital investigations and cause a lot of evidence to be lost. Moreover, it does not incentivize courts to create precedent explaining when exactly a mosaic search is triggered within the scope of a digital investigation.

In theory, the greater deterrent effect that an all-or-nothing exclusionary rule carries will cause police officers to act more carefully when thinking about what surveillance techniques they use.[160] By making all evidence in an unwarranted mosaic search excludable, the hope is that the government will get a warrant every time it wants to engage in long-term digital surveillance.[161] Thus, the key with this all-or-nothing deterrent is that when a government officer who is considering surveilling a suspect faces an ambiguous standard, and the potential consequence for breaching the standard undermines the whole reason he or she wants to engage in such surveillance in the first place (acquiring evidence to secure a conviction), the reasonable government officer will err on the side of restricting the surveillance in some way or getting a warrant.

The problem with the enhanced deterrent of the all-or-nothing approach is that it would lead to a lot of lost evidence. It is particularly harsh because the application of the exclusionary rule would put the government in a worse position than it would have been in if it did not violate the suspect's rights altogether, forcing it to investigate digital information at its own peril.[162] For example, if the government subpoenaed ten days of CSLI, and the court held the mosaic search occurred on day seven, the government would have otherwise been entitled to just under seven days of this CSLI if it had limited its search accordingly. However, under the all-or-nothing approach, the government would not be able to use any of this digital evidence to convict the suspect.[163]

160. *See* Dworkin, *supra* note 29, at 332. ("If the exclusionary rule is to deter unlawful police conduct, then it must be harsh enough to make policemen notice and fear it and inflexible and certain enough in its application to preclude the possibility of avoiding the sanction and hence the temptation to try.").

161. The harsher application of the exclusionary rule in the "all-or-nothing" approach may actually be necessary to ensure law enforcement's adherence to the principles in *Carpenter*. *See id.*

162. Moreover, if the Court wanted to over-deter these searches, it probably instead should just endorse the source rule, which fits better into its existing doctrine.

163. Kerr describes how this issue could lead to complications when trying to simultaneously apply the "fruit of the poisonous tree" and "inevitable discovery" doctrines:

> [I]magine the police learn on day two of the ongoing surveillance that the suspect committed a crime. Should the evidence from day two be suppressed because it was part of the mosaic triggered after seven days, even though the collection of that evidence was not a search when it occurred? Or is the evidence from day two an inevitable discovery because it would have been discovered if the monitoring had stopped before the amount of monitoring crossed the mosaic threshold?

The harshness of the all-or-nothing approach could make courts reluctant to apply the exclusionary rule, leading to the implicit under-deterrence of mosaic searches. Judges do not enjoy using the exclusionary rule because it may set a guilty person free.[164] Thus, judges may be inclined to try to fit the facts of the case they are dealing with within an exception to the exclusionary rule rather than exclude all of the evidence from the would-be mosaic search.

Although the all-or-nothing approach is slightly simpler to apply, it may lead to the creation of more doctrinal ambiguities because courts would not have to determine the exact point when the government's surveillance activities crossed the mosaic threshold. After all, determining that the government's actions invaded a reasonable expectation of privacy and determining when exactly that invasion occurred within the scope of its investigation require slightly separate analyses.[165] However, if courts were to avoid precisely determining when a search occurred—as the *Carpenter* Court did[166]—it would be at the expense of doctrinal clarity, undermining one of the main reasons the mosaic theory was preferable to the source rule in the first place.[167]

2. The "After-Search" Approach

Another way the exclusionary rule could apply when a mosaic search occurs entails excluding only the evidence found after the point where the mosaic threshold was crossed.[168] This after-search approach avoids the potential over-deterrent effects of the all-or-nothing approach, leading to the preservation of more evidence. But, in practice, it may incentivize the government to make broad subpoena requests.

The primary advantage of the after-search approach is that the harshness of exclusion is narrowly tailored only to the evidence that the government could not have collected constitutionally. The after-search approach does not impose a complete bar on access to digital information secured in a mosaic search. This is in contrast with the all-or-nothing approach, which is problematic because it excludes evidence that the government could have

Kerr, *supra* note 21, at 343.

164. *See Hudson*, 547 U.S. at 591.

165. *See* Totenberg, *supra* note 89.

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

167. *See supra* Section II.B.2 (arguing the mosaic theory's main advantage is that it tethers the warrant requirement to actual privacy invasions).

168. Chief Justice Roberts, by adding in a footnote that seven days of location information would result in a Fourth Amendment search, *Carpenter*, 138 S. Ct. at 2217 n.3, may be indicating that this is the path the Court will take in the future.

used at trial if it were not for the broadness of its requests. With the after-search approach, the government would be able to use all the information it could have gathered constitutionally at trial.[169]

On the other hand, the after-search approach does not really deter the government from making broad requests for digital metadata when the amount of information they can request is ambiguous. If the after-search approach were employed, government agents looking to craft subpoena requests would be incentivized to make broad requests for information to guarantee the receipt of the maximum amount of information that would be admissible at trial. If the government agents make a broad request, they would still be allowed to use the information from the request that was uncovered before the mosaic search occurred. However, if the government agents narrowly estimated the amount of information that would be constitutionally allowed when facing an ambiguous standard, they would risk leaving valuable digital information on the table.

C. HOW SHOULD THE EXCLUSIONARY RULE APPLY?

The debate between the all-or-nothing and after-search approaches is one between two imperfect options. If these were the only two options, courts would essentially be forced to decide whether to over-deter mosaic searches with the all-or-nothing approach or under-deter them with the after-search approach.[170] This Section proposes a compromise between the two approaches outlined above and attempts to reconcile their respective failings. The proposed after-act approach requires courts to exclude all the evidence gathered by the government act that triggers a mosaic search and any subsequent act thereafter.[171] To illustrate this, if the government issued two subpoenas to track a suspect's whereabouts, each for five days of CSLI, and a hypothetical court held, for the first time, that the mosaic search definitively occurred on day seven, then only the second subpoena would be excluded because it was the single act that crossed the mosaic threshold.

The after-act approach deters sweeping government actions that acquire invasive amounts of digital information by incentivizing the government to structure its digital investigations in smaller batches to preserve as much evidence for trial as possible. This structure is advantageous because it

169. It is not unreasonable to imagine a future in which investigations are done entirely digitally; the after-search approach allows the police to engage in some minimal form of digital investigation without first getting a warrant.

170. Courts could adopt the source rule and avoid these issues.

171. Although this rule may not seem intuitive at first, the Court has discretion to adopt this approach given that the exclusionary rule is prophylactic.

makes government actors more conscious of their decisions, facilitates judicial review, focuses the exclusionary rule's attention on government decision points, and imposes an added efficiency cost on warrantless requests for digital information.

In cases like *Jones* and *Carpenter*, the after-act approach would require the exclusion of all evidence gathered by the government, but this is not necessarily an unjust outcome. These cases involve the government accessing vast amounts of digital information on a given suspect without a warrant in a single sweeping action and therefore are exactly the kinds of cases where the exclusionary rule should apply robustly.[172] In *Carpenter* and *Jones*, respectively, the government officers accessed 127 days' worth of CSLI from *a single subpoena* and 28 days' worth of GPS data from *the single act* of placing a tracking system on the suspect's car. Everything from these acts would be excluded given that the subpoena request and the placing of the GPS tracker on the defendant's car were the government acts that violated the respective suspects' reasonable expectations of privacy.

Accordingly, the after-act approach would incentivize the government to request digital information on a suspect in smaller batches to avoid the exclusion of any evidence they received in a request made before the mosaic threshold is crossed. In other words, the government could artificially structure its investigations to contain several distinct actions to insulate as much evidence as possible from the exclusionary rule. Consider the fictional example in which a court in a previous case decided the mosaic threshold rests at seven days of CSLI acquired. However, in a new case, the government is trying to access a more accurate and thus slightly more intrusive type of CSLI information—called CSLI 2.0—to track a suspect's movements. In theory, because CSLI 2.0 is more intrusive and accurate, it should likely be able to create a mosaic of the suspect's movements in less time. If courts were to apply the after-act approach, government agents would likely first try to subpoena and review a few days of CSLI 2.0 before

172. *Carpenter*, 138 S. Ct. at 2222 ("CSLI is an entirely different species of business record—something that implicates basic Fourth Amendment concerns about arbitrary government power much more directly than corporate tax or payroll ledgers."). While the Supreme Court in recent years has gone to great lengths to limit the application of the exclusionary rule, *see, e.g.*, Davis v. United States, 564 U.S. 229, 240–41 (2011) (applying the good-faith exception to the exclusionary rule), the Court has also been extremely protective of digital privacy in its two recent landmark Fourth Amendment cases, exhibiting its concerns that the government is gaining too much surveillance power, *see Carpenter*, 138 S. Ct. at 2214–17; Riley v. California, 573 U.S. 373, 386 (2014). Therefore, it is not implausible to expect the Court to robustly apply the exclusionary rule to mosaic searches because the mosaic theory vindicates twenty-first century privacy norms.

subpoenaing more in the face of this ambiguous standard.[173] This is because if the government does cross the mosaic threshold in their later subpoenas, all evidence uncovered in their initial subpoenas would still be admissible.

The after-act approach would thus force the government to be more cognizant of its digital-surveillance activities. Imagine in the preceding example that the government wanted the CSLI 2.0 information on the suspect because it had reason to believe the suspect robbed two banks. The government, under the after-act approach, would likely want to request the data that will be most pertinent to their investigation first to make sure that it was not excluded. In this example, the government could request CSLI 2.0 from the two days in which the robberies occurred. Then, after reviewing the information to determine that the suspect was present at the robberies, the government could request more ancillary information in subsequent subpoenas.[174] For example, it could request CSLI 2.0 to show what the suspect was doing during the days before each robbery to see where he or she frequented, to look for potential accomplices or witnesses, and so forth.

These decision points that the government would create under this approach sequentially structure the inflow of evidence, facilitating judicial review. In the context of the previous example, a court reviewing the government's investigatory techniques would have a sequence of subpoenas to look at to determine the point where the government violated the suspect's reasonable expectations of privacy.[175] Therefore, the inflow of evidence would be structured in a manner that resembles the sequential approach that is familiar to courts. Moreover, the after-act approach is doctrinally sound because the exclusionary rule aims to deter government misconduct, and this creates a record of government decision points. Rather than look at when a government action hoovers up too much digital information, courts can focus in on when the government makes the underlying decisions.

The after-act approach also imposes an efficiency cost on the government's choice between expending effort to break up its investigation into smaller pieces or to get a warrant. Returning to the same example discussed above, if the government were to make several requests for CSLI

173. Of course, this assumes that the government subpoenas one batch of information, reviews it, and then subpoenas the next batch, rather than submitting all seven subpoenas at once. If the government were to simply issue several subpoenas at once, courts would likely have to consider them as a single government act. This approach is not intended to simply burden the police with extra paperwork, but rather to force them to carefully narrow their requests for digital information.

174. Or alternatively, the government might have probable cause at this point to get a warrant for the rest of the information depending on the circumstances.

175. This could make it easier for courts to articulate durational limits in the first place.

2.0 on a given suspect from various phone companies, it would be much more time-consuming. Not to mention the government would have to deal more frequently with the third-party companies it is subpoenaing the information from—many of these companies actively review, challenge, and seek to narrow the requests they receive to protect their users' privacy.[176] Still, making several subpoena requests for CSLI does not require as much effort as investigating suspects in non-digital ways, as it is likely still more expensive to have police officers follow suspects around all day. The after-act approach incentivizes government agents to spend that additional effort to go get a warrant, especially if they are dealing with the possibility of violating ambiguous standards, which could lead to the fruits of their investigations being excluded at trial.

CONCLUSION

The Supreme Court's recent *Carpenter* ruling foreshadowed a shift in its understanding of the Fourth Amendment in the digital age while leaving a mess of questions in its wake—including how to determine when a *Carpenter* search occurs. This Note compared the source rule and the mosaic theory, which are two possible methods that provide an answer to this very question. Of the two, the mosaic theory better tethers the warrant requirement to actual invasions of people's reasonable expectations of privacy in their digital footprint. On the other hand, the mosaic theory may be overlooked by courts because, unlike the source rule, it does not fit seamlessly into the Court's existing search doctrine.

This Note attempted to answer one question that the mosaic theory would require courts to grapple with if it were adopted: how to best apply the exclusionary rule when a mosaic search occurs. Of the three approaches this Note discussed, the after-act approach is the superior one. It deters the government from making broad subpoena requests for third-party digital information by putting the ball in the government's court to break up its requests in order to limit its exposure to the exclusionary rule. Moreover, by incentivizing the government to make several subpoena requests for digital information, the after-act approach creates a sequence of government decision points, making it easier for judges to review.

176. *See, e.g.*, *About Our Practices and Your Data*, MICROSOFT, https://blogs.microsoft.com/datalaw/our-practices/#Why-screen-government-requests-customer-data [https://perma.cc/V6BE-FFE6] (describing how Microsoft assesses and challenges the subpoenas and warrants it receives from the government); *Legal Process for User Data Requests FAQs*, GOOGLE, https://support.google.com/transparencyreport/answer/7381738?hl=en [https://perma.cc/GLS6-CVAH] (describing how Google assesses and challenges the subpoenas and warrants it receives from the government).

Ultimately, this Note deals with a very narrow question and its analysis is useful to both proponents of the mosaic theory and the source rule. For those who favor the mosaic theory, it leaves courts with a reasonable answer to the mosaic theory's exclusionary problem: the after-act approach. Alternatively, it illustrates the depth of analysis that would be needed to answer the remaining doctrinal wrinkles that the mosaic theory would present if adopted. These questions could be avoided under the source rule.