Loyola of Los Angeles
Entertainment Law Review

Volume 40 | Number 1 Article 1

Fall 12-4-2019

Attempts Towards a Zero-Sum Game: A Recurring Imbalance Between Individual Privacy and the Fourth Amendment

Christopher Netniss
LMU Loyola Law School, Los Angeles, christopher.netniss@lls.edu

ATTEMPTS TOWARDS A ZERO-SUM GAME: A RECURRING IMBALANCE BETWEEN INDIVIDUAL PRIVACY AND THE FOURTH AMENDMENT

Christopher N. Netniss[*]

The digital era we live in today allows society to work, shop, socialize, and even monitor one's health without having to leave the confines of one's home. In a recent landmark privacy case, *Carpenter v. United States*, the individual privacy implications of the Fourth Amendment were strengthened when the Supreme Court held that the government must generally obtain a warrant before collecting more than six days of historical cell-site location information from a third-party service provider, like Verizon. Cell-site location information could implicate numerous Fourth Amendment concepts, such as the third-party doctrine, mosaic theory, and public exposure doctrine. Refusing to apply the third-party doctrine in its existing state, the Supreme Court advanced an alternative digital third-party doctrine to protect historical cell-site location information.

Recognizing the technological advances and the ubiquitous use of technology by society, the Court's decision attempts to balance the playing field between individual privacy and law enforcement. This Article explores the Supreme Court's selective valuation of privacy in physical and digital information. In doing so, this Article argues that a digital third-party doctrine will not resolve the tension between the Fourth Amendment and technology, as it is a direct departure from traditional expectations and proves unworkable. What will prove workable, however, is adhering to the common understanding that what enters the public—either through physical or digital information—remains public knowledge, and that which is public knowledge does not amount to a reasonable expectation of privacy.

---

[*] J.D. Candidate, 2020, Loyola Law School, Los Angeles. The author would like to first thank his parents for their unconditional love and endless wisdom. The author would also like to thank his advisor, Professor Marcy Strauss, whose insight and feedback improved this piece immeasurably, and his student Note advisors for providing feedback and encouragement no matter the time of day. Finally, the author would like to express his gratitude to his team at the *Loyola of Los Angeles Entertainment Law Review* for the honor of working with them.

> How much are you willing to give up for your privacy? Are you willing to forego social media? Are you willing to limit your conversations with family and friends to in-person only? Are you willing to operate your own personal banking system at home instead of using a conventional banking method? Are you willing to disconnect your cell phone each time you travel outside the confines of your home? Are you willing to physically travel to a convenience store to inquire about a product instead of using your electronics to browse their website online?

I. INTRODUCTION

Imagine having the sudden urge to watch a baseball game at Dodger Stadium in Los Angeles, California. Using your cell phone, you start researching when the next Dodger game is. You find out the Dodgers have a home game that night, so you scour the Internet for tickets, visiting site after site for the best bargain. You end up finding the right seat at the right price, prompting you to pull out your banking debit card to finalize the purchase. An e-mail confirmation is then sent to you, and you begin making your way to Dodger Stadium. Along the way, you get hungry. You stop at a local restaurant, purchase food with your debit card, then continue on your way to the stadium. You get to the stadium, and in order to enter the stadium, you show security the e-mail confirmation from your phone. Once inside the stadium, you purchase drinks and a Dodger hat using your debit card. Excited, you share photos of yourself at the stadium on Facebook. After the game, you use a navigational app on your phone, Waze, to help get you home faster. Finally, you arrive home, satisfied that you acted on your idea to watch a baseball game. Unfortunately for you, what began as an idea in attending a baseball game is now a lasting digital trail of your physical whereabouts. And until recently, you lacked an expectation of privacy in your personal information that law enforcement wants to collect from your journey to Dodger Stadium. That may have changed in *Carpenter v. United States* ("*Carpenter*").[1]

In *Carpenter*, a recent landmark privacy case, the individual privacy implications of the Fourth Amendment were strengthened when the United States Supreme Court held that the government must generally obtain a warrant in order to collect historical cell-site location information (CSLI) from

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

a third-party service provider.[2] Using the example above, each time the Dodger fan's cell phone was near a cell tower, a signal would transmit to the cell tower generating an approximate location of the cell phone, and the location history of the cell phone would then be documented and stored by a third-party service provider.[3] If, a week later, law enforcement approaches Verizon, a third-party service provider, with a subpoena requesting the location information generated by the Dodger fan's cell phone, the Supreme Court's holding in *Carpenter* may give the Dodger fan a legitimate expectation of privacy in the location information that was generated.[4] The same could not be said if law enforcement went to the Dodger fan's bank with a subpoena and requested the fan's bank records, detailing the fan's transactional history.[5] While the fan may have a privacy interest in the location information generated by the cell towers, the fan has no privacy interest in the bank records.[6]

The Fourth Amendment,[7] originally enacted to protect against trespass in the home by law enforcement, today also safeguards digital data from being obtained by law enforcement. The market for technology and the "seismic shifts in digital technology" cause a recurring imbalance between individual privacy and the Fourth Amendment.[8] This Article explores the privacy implications of both digital data and physical information, and explains the similarities and differences of the privacy interests between the

2. *Id.* at 2221 (holding that "the Government must generally obtain a warrant supported by probable cause before acquiring" historical cell-site location information from third-party providers).

3. *See, e.g.*, State v. Earls, 70 A.3d 630, 636–37 (N.J. 2013) (explaining how cell-site location information is generated).

4. *Carpenter*, 138 S. Ct. at 2221 (holding that "the Government must generally obtain a warrant supported by probable cause before acquiring" historical cell-site location information from third party providers).

5. United States v. Miller, 425 U.S. 435, 444 (1976) (holding that "the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights" of an individual).

6. *Id.*; *Carpenter*, 138 S. Ct. at 2221.

7. U.S. CONST. amend. IV.

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

two. In doing so, this Article explores numerous Fourth Amendment concepts such as the third-party doctrine (TPD), the mosaic theory, and the public exposure doctrine (PED).

Part II of this Article describes the legal background of the Fourth Amendment and the background from which *Carpenter* draws its authority. Part III examines the *Carpenter* decision. Part IV explains the implications of obtaining digital data and physical information, and why the third-party doctrine proves unworkable, especially considering that today's physical information is increasingly digitized. Part V discusses the impracticability of factoring length of surveillance into the reasonable expectations of privacy analysis. Finally, Part VI concludes this Article by advocating that both the third-party doctrine and the mosaic theory should be rejected, while adhering to the common understanding that public knowledge does not amount to a legitimate expectation of privacy when it enters the public eye.

II. BACKGROUND OF THE LEGAL STANDARD

The ratification of the Fourth Amendment was a direct departure from the once-utilized "Writs of Assistance."[9] These general, non-specific warrants had arbitrary roots, which carved the path for the Fourth Amendment.[10] Fourth Amendment jurisprudence protects individuals from being subject to an unreasonable search or seizure by the government.[11] As the first clause of the Fourth Amendment guards against "unreasonable" searches or seizures, reasonableness has been coined the "fundamental command" of the Fourth Amendment.[12] This "imprecise and flexible term" reflects the framers' recognition "that searches and seizures were too valuable to law enforcement to prohibit them entirely," and instead "should be slowed down."[13]

---

9. James Otis, *Against Writs of Assistance*, CONST. SOC'Y (Feb. 24, 1761), https://www.constitution.org/bor/otis_against_writs.htm [https://perma.cc/PQG2-W4Z5].

10. *See, e.g.*, Stanford v. Texas, 379 U.S. 476, 481–82 (1965) (expressing that "the Fourth Amendment was most immediately the product of contemporary revulsion against a regime of writs of assistance . . . .").

11. U.S. CONST. amend. IV. The Fourth Amendment's plain text affords "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," such that "no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

12. New Jersey v. T.L.O., 469 U.S. 325, 340 (1985).

13. Berger v. New York, 388 U.S. 41, 75 (1967) (Black, J., dissenting).

While the expectations of society helped create the Fourth Amendment, the expectations of society continues, for better or worse, to alter the protections of the Fourth Amendment. Today's example is the booming nature of technology.

A. Search: Differentiating Between its Conventional and Constitutional Use

Before delving into the many legal canons that are connected to the Fourth Amendment, it is important to differentiate between a Fourth Amendment "search," and the conventional everyday use of the word. While we all may have searched the couch for our misplaced car keys, the remote to the television, or even a shoe that our dog might have hidden, a Fourth Amendment "search" has a different meaning.[14]

A modern Fourth Amendment "search" is driven by two separate tests—both of which—individuals can assert. The first is the common-law trespass test invoked in *United States v. Jones* ("*Jones*"), which guards against the warrantless and physical intrusion of private property by law enforcement "for the purpose of obtaining information."[15] The second test, which this Article primarily focuses on, was invoked in *Katz v. United States* ("*Katz*").[16] In *Katz*, the Supreme Court addressed the constitutionality of an electronic listening and recording device attached to a public telephone booth by the government without a warrant.[17] Both Katz and the government argued the constitutionality of the public telephone booth in terms of a property interest,[18] but the Court was instead concerned with individual privacy.[19] The government argued that Katz entered a public telephone booth that was

---

14. *See generally* Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979 (2011) (explaining the structure and evolution of the Fourth Amendment).

15. United States v. Jones, 565 U.S. 400, 404–05 (2012) (holding that "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'").

16. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *Jones*, 565 U.S. at 408–09 ("[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.").

17. *Katz*, 389 U.S. at 348, 354–56.

18. *Id.* at 351.

19. *Id.* at 351–52.

constructed out of glass, allowing any passerby, including a government official, to observe Katz.[20] The Court agreed with the government insofar as "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[21] But the Court disagreed that this rule is absolute.[22] The Court explained that when Katz entered the public telephone booth, closed the door behind him, paid the price to make a phone call, and only spoke loud enough for the recipient of the call to hear him, Katz sought to exclude the "uninvited ear," not the "intruding eye."[23] For this reason, Katz had an expectation that "the words he utters" would remain private,[24] and because the government did not obtain a warrant prior to recording Katz' conversation,[25] the government violated Katz' Fourth Amendment privacy right.[26] As Katz successfully did, individuals can invoke the protections of the Fourth Amendment by demonstrating an "actual (subjective) expectation of privacy" that society recognizes as reasonable.[27] This two-part test encompasses a subjective and objective prong, but courts tend to place much more weight on the objective prong.[28] The Supreme Court has emphasized that the reasonable expectations of privacy

20. *Id.* at 352.

21. *Id.* at 351.

22. *See, e.g.*, *id.* at 352 (explaining that Katz "did not shed his right to [privacy] . . . simply because he made his calls from a place where he might be seen.").

23. *See id.* at 352.

24. *Id.* (noting that Katz had an expectation "that the words he utters into the mouthpiece will not be broadcast to the world."); *id.* at 361 (Harlan, J., concurring).

25. *Id.* at 354–57 (majority opinion); *id.* at 361 (Harlan, J., concurring).

26. *Id.* at 358–59 (majority opinion).

27. *Id.* at 361 (Harlan, J., concurrence).

28. *See generally* Orin S. Kerr, *Katz Only Has One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113 (2015) (statistically analyzing how a large majority of courts consider and decide cases with little-to-no assessment of the subjective prong); *see also* Orin S. Kerr, *Applying the Fourth Amendment to the Internet*, 62 STAN. L. REV. 1005, 1037 (2010) [hereinafter *Fourth Amendment & the Internet*] (expressing that "the phrase 'reasonable expectation of privacy' is essentially a legal fiction that masks a normative inquiry into whether a particular law enforcement technique should be regulated by the Fourth Amendment.").

test asserted in *Katz* is subject to certain exceptions, like the third-party doctrine and the public exposure doctrine.[29]

B. Third-Party Doctrine (TPD): Traditional Rule

The third-party doctrine originated in *United States v. Miller*[30] and was reinforced in *Smith v. Maryland*,[31] where the Supreme Court established that individuals lack any legitimate expectation of privacy in information voluntarily disclosed to third parties.[32] For example, suppose Will enters a bank, creates an account, and later makes purchases using a debit card that was issued to him from his bank. In this example, the bank is the third party, and all of Will's transactions serve as information that Will voluntarily shares with the bank. If the government sought to obtain a hard copy of Will's transactional history from the bank, Will has no privacy interest in those bank records despite the records being a summary of when, where, and how Will used his money. The reason for Will's lack of privacy interest is simple, yet difficult to accept. When individuals voluntarily convey information to third parties, it is presumed that they assume the risk that the third party will then disclose that information to the government.[33] Even if an individual is unaware that his information is being documented and stored by a third party, the application of the traditional third-party doctrine does not change because the traditional rule does not cater to the "least-sophisticated" consumer.[34] Although the presumption that individuals assume the risk remains

29. *See Katz*, 389 U.S. at 357 (Harlan, J., concurring) (emphasizing the two-prong privacy test is "subject only to a few specifically established and well-delineated exceptions.").

30. *See* Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) (explaining that the "third party doctrine largely traces its roots to" United States v. Miller, 425 U.S. 435 (1976)).

31. Smith v. Maryland, 442 U.S. 735, 742–44 (1979).

32. United States v. Miller, 425 U.S. 435, 442–43 (1976). For a detailed analysis of the third-party doctrine, see generally Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009) [hereinafter *Third-Party Doctrine*] (exploring the third-party doctrine).

33. *Miller*, 425 U.S. at 443; *see also Smith*, 442 U.S. at 745.

34. United States v. Carpenter, 819 F.3d 880, 887 (6th Cir. 2016); *see Smith*, 442 U.S. at 742; *see also Miller*, 425 U.S. at 443 (emphasizing that the lack of privacy interest remains true "even if the information is revealed on the assumption that it will be used only for a limited purpose.").

true under the traditional third-party doctrine,[35] there are circumstances where courts do assess the content of information.

1. Content Information Versus Non-Content Information

When analyzing the third-party doctrine, courts often assess whether the information voluntarily shared contains content information or non-content information.[36] Content information is the actual "contents of communications,"[37] such as the typed message in an email or text message,[38] or the written message on a letter that is sealed inside an envelope.[39] These type of communications often reveal an individual's personal and private thoughts.[40] The Supreme Court and its progeny have held that individuals have an expectation of privacy in content information—and as a result, the government must generally obtain a warrant supported by probable cause in order to obtain content information.[41] Non-content information, however, is the out-

35. *Miller*, 425 U.S. at 443; *see also Smith*, 442 U.S. at 745.

36. *See generally Fourth Amendment & the Internet*, *supra* note 28 (explaining the distinction between content information and non-content information, and how courts assess the two).

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

38. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding that individuals have a reasonable expectation of privacy in the content of their emails); City of Ontario v. Quon, 560 U.S. 746, 754–55 (2010) (discussing the expectations of privacy in the content of text messages).

39. *Ex parte* Jackson, 96 U.S. 727, 733 (1878) (holding that "[l]etters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles.").

40. *Fourth Amendment & the Internet*, *supra* note 28, at 1020–22.

41. *Ex parte Jackson*, 96 U.S. at 733 ("The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household."); *see also Warshak*, 631 F.3d at 288 (holding that individuals have a reasonable expectation of privacy in the content of their emails).

ward information necessary to establish communication, such as a recipient's address on an envelope.[42] Because non-content information is information that is shared with third parties, like the postal office when a letter is mailed, the government does not need a warrant supported by probable cause to obtain the non-content information contained on the envelope.[43]

Courts have also analyzed content information and non-content information in e-mail communications.[44] Although lower courts have instructed that the actual content of e-mail communications is protected,[45] the Supreme Court has made clear that digital communication is not completely immune from being obtained and read without a warrant.[46] At the same time, if the same communication is written on paper, placed in an envelope, sealed, and placed in the mail for delivery, then the letter carries with it the full protection of the Fourth Amendment.[47] The implications of digital and physical information lead to a recurring issue: different forms of communication carry different constitutional protections despite containing the same information.

---

42. *See, e.g.*, *Smith*, 442 U.S. at 741 (explaining that a pen register does not reveal the content of a phone call, but the phone numbers dialed as "a means of establishing communication."); *see also Ex parte Jackson*, 96 U.S. at 733 (holding that "[l]etters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles.").

43. *See Smith*, 442 U.S. at 741.

44. *See, e.g.*, *Warshak*, 631 F.3d at 285–88.

45. *See, e.g.*, *Warshak*, 631 F.3d at 288 (holding that individuals have a reasonable expectation of privacy in the content of their emails).

46. *See* City of Ontario v. Quon, 560 U.S. 746, 762 (2010) (emphasizing that "[e]ven if he could assume some level of privacy would inhere in his messages, it would not have been reasonable for Quon to conclude that his messages were in all circumstances immune from scrutiny.").

47. *E.g.*, *Ex parte Jackson*, 96 U.S. at 733 ("Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household.").

C. Public Exposure Doctrine

The public exposure doctrine is fairly intuitive: what an individual exposes to the public, he lacks an expectation of privacy in.[48] This rule is not absolute, as not every public exposure vitiates Fourth Amendment protection.[49] A prime example is the central telephone booth case, *Katz v. United States*, where the Supreme Court recognized the expectations of privacy when individuals are in public.[50] Although the Court emphasized that "objects, activities, or statements that [a person] exposes to the 'plain view' of outsiders" do not receive Fourth Amendment protection,[51] the Court counteractively noted that "what [one] seeks to preserve as private, even in an area accessible to the public, may [still] be constitutionally protected."[52] While in public, Katz stepped inside a public telephone booth, closed the door behind him, paid the fee to make a call, and began communicating.[53] Left with analyzing the constitutional protection of public observation, the Court expressed that it was not the "intruding eye"[54] that warranted an expectation of privacy for Katz; it was the "uninvited ear."[55] Katz' deliberate attempt to keep his phone call private meant that Katz had an expectation "that the words he utters into the mouthpiece will not be broadcast to the world," and this expectation is one that society agreed with.[56]

---

48. *E.g.*, United States v. Knotts, 460 U.S. 276, 281–82 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").

49. Katz v. United States, 389 U.S. 347, 351–52 (1967) (explaining that "what a person seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

50. *Id.* at 350–51.

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

52. *Id.* at 351–52 (majority opinion).

53. *Id.* at 352 ("One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."); *id.* at 361 (Harlan, J., concurring).

54. *Id.* at 352 (majority opinion).

55. *Id.*

56. *Id.*

Vehicles are also subject to the public exposure doctrine.[57] When vehicles are "thrust[ed] into the public eye,"[58] on first impression, the public exposure doctrine leads us to believe that simply observing the vehicle is not a Fourth Amendment search.[59] But this is not always true. One example stems from "longer term" monitoring by law enforcement.[60] Regardless if a vehicle is "disclosed to the public at large,"[61] depending on how long law enforcement officials observe the vehicle, they could violate the Fourth Amendment.[62]

1. Length of Surveillance

The Supreme Court has underscored the point that society does not expect that law enforcement would (or could) expend the time, resources, and money to monitor and catalogue every detail about an individual for long periods of time.[63] The Supreme Court has also expressed concern that lengthy surveillance has the capability of revealing an abundance of personal information about an individual.[64] Revealing large quantities of personal information is not what society expects to volunteer to the general public when traveling in public.[65] As Justice Ginsburg put it:

---

57. *See, e.g.*, New York v. Class, 475 U.S. 106, 114 (1986); United States v. Knotts, 460 U.S. 276, 281 (1983); United States v. Jones, 565 U.S. 400, 412 (2012).

58. *Class*, 475 U.S at 114.

59. *See, e.g.*, *Class*, 475 U.S at 114 (referring to a vehicle, "to examine it does not constitute a [Fourth Amendment] search.").

60. *Jones*, 565 U.S. at 415 (Alito, J., concurring in judgment); *id.* at 430 (Sotomayor, J., concurring).

61. Carpenter v. United States, 138 S. Ct. 2206, 2215 (2018); *see Jones*, 565 U.S. at 415 (Sotomayor, J., concurring); *see also id.* at 430 (Alito, J., concurring in judgment).

62. *See, e.g.*, *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring); *id.* at 430 (Alito, J., concurring in judgment).

63. *Carpenter*, 138 S. Ct. at 2217 (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring in judgement) ("[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.")).

64. *See, e.g.*, *Jones*, 565 U.S. at 415–16 (Sotomayor, J., concurring).

65. *Id.* at 416; *id.* at 430 (Alito, J., concurring in judgment).

> The whole of one's movements over the course of a month is not constructively exposed to the public because, like a rap sheet, that whole reveals far more than the individual movements it comprises. The difference is not one of degree but of kind, for no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life.[66]

The aggregation of this information creates a "mosaic."[67] The so-called mosaic theory is "premised on aggregation: it considers whether a set of non-searches aggregated together amount to a search because their collection and subsequent analysis creates a revealing mosaic."[68] The Supreme Court explains that analyzing information in the aggregate has the potential to reveal "the sum of one's public movements" that could not be reasonably discoverable by the general public.[69] In other words, what the public observes in a short length of time does not compare to the revealing nature of a longer observation by law enforcement.[70]

For example, if Bella goes to the grocery store on Monday, the public may observe the streets Bella drives on, the route Bella takes to the grocery store, the name of the grocery store, and perhaps the address of Bella's home. Now suppose law enforcement followed Bella for seven days straight. Law enforcement could observe much more information concerning: (1) where Bella shops; (2) where Bella works; (3) where Bella eats; (4) what Bella does on the weekends; and (5) who Bella associates with. Narrowing in on "aggregation," it follows that any particular investigation could run afoul of the

---

66. United States v. Maynard, 615 F.3d 544, 561–62 (D.C. Cir. 2010).

67. *See generally* David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628 (2005) (noting that the term "mosaic," is a "borrowed [term] from national security law.").

68. *See generally* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012) (explaining the implications of the mosaic theory).

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

70. *See, e.g.*, Gabriel R. Schlabach, *Privacy in The Cloud: The Mosaic Theory and the Stored Communications Act*, 67 STAN. L. REV. 677, 678–79 (2015) (explaining that "[u]nder this theory, certain types of long-term (or otherwise expansive) surveillance violate a suspect's reasonable expectation of privacy, even when each individual act of surveillance would otherwise pass Fourth Amendment muster, because the government can analyze the information in the aggregate to infer private details about the suspect that no individual member of the public could reasonably discover by observing her for a short time.").

Fourth Amendment depending on the length of surveillance.[71] One wonders, how long is *too* long?[72] And how much information is *too* much information? To date, the Supreme Court has yet to establish an exact demarcation line separating long term surveillance from short term surveillance.[73] Still, the Court continues to exploit the duration of law enforcement surveillance, including the technology used by law enforcement when surveilling.

2. Technology Employed by Law Enforcement

The means by which law enforcement obtains information from individuals continues to, and perhaps for good reason, face scrutiny by the Supreme Court.[74] Depending on the cost, ease, and efficiency of obtaining information, law enforcement could run afoul of the Fourth Amendment.[75] But how can cost, difficulty, and efficiency influence the Supreme Court's decision?[76] One reason offered is that the methods by which law enforcement

71. *See* Kerr, *supra* note 68, at 343–49 (advocating that "courts should reject the mosaic theory.").

72. Orin S. Kerr, *When Does a Carpenter Search Start—and When Does It Stop?*, LAWFARE (July 6, 2018, 10:24 AM), https://www.lawfareblog.com/when-does-carpenter-search-start-and-when-does-it-stop [https://perma.cc/63QN-KBDF].

73. *See, e.g.*, *Jones*, 565 U.S. at 430 (Alito, J., concurring in judgment) ("We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.").

74. *See, e.g.*, *id.* at 415–16 (Sotomayor, J., concurring) (citation omitted) (arguing that "because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'"); *see also* United States v. Maynard, 615 F.3d 544, 566 (D.C. Cir. 2010) (explaining that "when it comes to the Fourth Amendment, means do matter.").

75. Carpenter v. United States, 138 S. Ct. 2206, 2217–18 (2018) (explaining that "cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools.").

76. *See, e.g.*, *id.* at 2266 (Gorsuch, J., dissent) ("At what point does access to electronic data amount to 'arbitrary' authority? When does police surveillance become 'too permeating'? And what sort of 'obstacles' should judges 'place' in law enforcement's path when it does? We simply do not know.").

obtains information could disrupt the balance of societal expectations towards law enforcement's authority.[77] Another reason is that society does not expect that difficult, elaborate, and costly techniques will be employed by law enforcement in order to gather information on individuals.[78] Indeed, as more and more law enforcement agencies are using technology to track the physical whereabouts of individuals, there is a need to balance the playing field between what society expects and how law enforcement obtains information on society.[79] As one commentator points out, "[t]he law intentionally limits the scope of police power to limit the government's capacity for abusive practices."[80] This, perhaps, explains the Supreme Court's constant need to strike "a certain balance between government power and individual rights."[81]

77. *See, e.g.*, *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) (citation omitted) (explaining that "the government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse . . . [and] may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'").

78. *Id.* at 430 (Alito, J., concurring in judgment) ("'[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.'").

79. *See, e.g., When Does a Carpenter Search Start—and When Does It Stop?*, *supra* note 72 (explaining that because technology has made law enforcement's access to cell-site location information "easy and potentially very common, the law needs to step in and make that surveillance difficult and rare again.").

80. Orin S. Kerr, *An Equilibrium-Adjustment Theory of The Fourth Amendment*, 125 HARV. L. REV. 476, 485 (2011) [hereinafter *Equilibrium-Adjustment Theory*].

81. *Id.* at 485–86 (explaining that "[i]f both the law and police practice remain constant, the use of new tools to commit crimes will let wrongdoers commit more crimes and will correspondingly diminish police power to stop them. Of course, the police use new tools, too. For the police trying to solve crimes, new tools mean new ways to solve crimes. If the police use those new tools - and if the law allows the use of the new tools more readily than traditional methods to investigate the same offense - the new tools can expand government power by letting the government collect more information more easily than before.").

III. THE *CARPENTER* DECISION

After a slew of RadioShack and T-Mobile robberies in 2011,[82] prosecutors obtained two court orders under the Stored Communications Act,[83] compelling cellular telephone service providers MetroPCS and Sprint to turn over historical cell-site location information of Timothy Carpenter.[84] Unlike a search warrant which requires probable cause, the Stored Communications Act allows the government to compel the disclosure of certain telecommunications records when law enforcement shows reasonable grounds for believing that the records are "relevant and material to an ongoing criminal investigation."[85] This standard is substantially lower than the probable cause standard required of a warrant.[86] The cell-site records revealed that "Carpenter's phone was near" most of the robbery sites "'at the exact time'" the robberies took place.[87] Carpenter argued that the government violated the Fourth Amendment by obtaining the cell-site records without a search warrant supported by probable cause.[88] Despite contesting the means in which law enforcement obtained the cell-site location information, Carpenter was convicted.[89]

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

83. 18 U.S.C. § 2703(d) (2012). For a thorough analysis of the Stored Communications Act, see generally Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislature's Guide to Amending it*, 72 GEO. WASH. L. REV. 1208 (2004).

84. *Carpenter*, 138 S. Ct. at 2212 (One order sought MetroPCS records for 152 days of calls but yielded records spanning 127 days. The second order requested seven days of Sprint records but yielded data for two days. Together, the data provided prosecutors with "12,898 location points cataloging Carpenter's movements—an average of 101 data points per day.").

85. 18 U.S.C. § 2703(d).

86. *Carpenter*, 138 S. Ct. at 2221.

87. *Id.* at 2213 (citation omitted).

88. *Id.* at 2212.

89. *Id.* at 2212–13.

A. The Sixth Circuit Court's Ruling

On appeal, the Sixth Circuit Court of Appeals relied heavily on the traditional third-party doctrine in upholding Carpenter's conviction.[90] The court analyzed whether individuals assume the risk that their location history will be recorded and maintained. In doing so, the court emphasized that "any cellphone user who has seen her phone's signal strength fluctuate must know that, when she places or receives a call, her phone 'exposes' its location to the nearest cell tower and thus to the company that operates the tower."[91] Moreover, "any cellphone user who has paid 'roaming' (*i.e.*, out-of-network) charges—or even cellphone users who have not— should know that wireless carriers have 'facilities for recording' locational information and that 'the phone company does in fact record this information for a variety of legitimate business purposes.'"[92] The court refused to accept that the "least-sophisticated phone user"[93] may not know that their location information was being monitored, and instead re-affirmed the presumption that individuals assume such risks accompanied with sharing information with third parties.[94]

The court also distinguished between content information and non-content information, and explained that while "the content of personal communications is private, the information necessary to get those communications from point A to point B is not."[95] Cell-site data, according to the Sixth Circuit, is akin to the mailing addresses "that facilitate personal communications, rather than part of the content of those communications themselves."[96] Thus, the cell-site data in *Carpenter* concerned only non-content information, which did not require the government to obtain a warrant supported

90. United States v. Carpenter, 819 F.3d 880, 886–90 (6th Cir. 2016).

91. *Id.* at 888.

92. *Id.* (quoting Smith v. Maryland, 442 U.S. 735, 741–43 (1979)).

93. *Id.* at 887.

94. *Id.* at 887–88.

95. *Id.* at 886.

96. *Id.* at 887.

by probable cause because individuals have no privacy interest in non-content information.[97]

The Sixth Circuit also weighed in on the level of precision that cell-site location data reveals.[98] In doing so, the court distinguished cell-site data from data collected by a global positioning system (GPS).[99] The court emphasized that cell-site location information reveals an inexact location "within a 3.5 million square-foot to 100 million square-foot area—as much as 12,500 times less accurate" than GPS devices which "are accurate within about 50 feet."[100] Based on the increased level of accuracy that GPS data produces, GPS data can reveal precise details about an individual that could not be revealed by cell-site data.[101] As a result, the government's warrantless collection of historical cell-site data under the Stored Communications Act was permissible.

B. The United States Supreme Court's Ruling

On review, the United States Supreme Court, in a narrow 5-4 decision, held that the government's acquisition of historical cell-site location information was a Fourth Amendment search under *Katz*' reasonable expectation of privacy test.[102] Beginning with the Stored Communications Act, the Court refused to accept that law enforcement could obtain seven days' worth of historical cell-site location information using a court order under the Stored

---

97. *Id.* at 887–88 (explaining that cell-site location records "fall on the unprotected side of this line . . . [because] [t]hose records say nothing about the content of any calls. Instead the records include routing information.").

98. *Id.* at 889.

99. *Id.* (emphasizing that "the locational data here are accurate within a 3.5 million square-foot to 100 million square-foot area—as much as 12,500 times less accurate than the GPS data in *Jones*.").

100. *Id.* ("[Cell-site] data could do no better than locate the defendants' cellphones within a 120- (or sometimes 60-) degree radial wedge extending between one-half mile and two miles in length. Which is to say the locational data here are accurate within a 3.5 million square-foot to 100 million square-foot area—as much as 12,500 times less accurate than the GPS data in *Jones*.").

101. *Id.* at 886–90 (citation omitted) (explaining that unlike GPS data which "might tell a story of trips to 'the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on,' cell-site data cannot tell that story.").

102. Carpenter v. United States, 138 S. Ct. 2206, 2217–19 (2018).

Communications Act.[103] Instead, to obtain this information, the government must generally obtain a warrant.[104]

Next, the Court strengthened its stance on privacy by reaffirming the need to scale back law enforcement's ease in obtaining information on the public.[105] Obtaining cell-site location information, in the eyes of the Court, "is remarkably easy . . . and efficient" for law enforcement—and provides law enforcement with archived information about an individual "at practically no expense."[106] The Court explained that society does not expect to reveal a historical database to the world when venturing out in public, as opposed to exposing the single-day observances to public goers.[107] Thus, the government's acquisition of Carpenter's historical cell-site location information "invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements."[108]

Finally, the Court expressly rejected the viability of the third-party doctrine's use as applied to historical cell-site location information for at least two reasons. First, cell-site data is both qualitatively and quantitatively dif-

---

103. *Id.* at 2221–23 ("While police must get a warrant when collecting CSLI to assist in the mine-run criminal investigation, the rule we set forth does not limit their ability to respond to an ongoing emergency.").

104. *Id.* at 2221 ("Before compelling a wireless carrier to turn over a subscriber's CSLI, the Government's obligation is a familiar one—get a warrant.").

105. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 37 (2001) (addressing the common usage of thermal imaging technology, while emphasizing that "all details [in the home] are intimate details, because the entire area is held safe from prying government eyes."); United States v. Jones, 565 U.S. 400, 403 (2012) (addressing the unconstitutionality of law enforcement attaching a GPS on a vehicle and monitoring it for twenty-eight days); Riley v. California, 573 U.S. 373, 385–86 (2014) (addressing the ubiquity of cell phones and the vast quantity of data stored therein); *Carpenter*, 138 S. Ct. at 2206 (addressing the digital data stored by cell service providers from users' cell phones pinging to cell-site towers throughout their locale).

106. *Carpenter*, 138 S. Ct. at 2217–18 ("And like GPS monitoring, cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense.").

107. *See id.* (holding that "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.").

108. *Id.* at 2219.

ferent than the phone records and bank records collected in *Smith* and *Miller*.[109] In other words, cell-site data reveals more personal and intimate information, and the amount of information cell-site data reveals exceeds the single, day-to-day expectancies of society. Second, the Court underscored that individuals do not actually share their location information because "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[110] Because cell phones are considered absolutely necessary, it is not realistic to argue that individuals assume the risk that their location information will be documented, catalogued, and volunteered to third parties simply by carrying and using a cell phone in public.[111] *Carpenter* implicitly incorporates Justice Marshall's dissenting opinion, stating that "[i]t is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative."[112] *Carpenter* similarly pointed out that, "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data."[113] In *Carpenter*'s view, disconnecting a cell-phone to avoid cell-phone location tracking is an unreasonable alternative that could not be expected of society. Although *Miller* and *Smith* hold that, under the traditional third-party doctrine, individuals have *no* expectation of privacy in information voluntarily shared with another, based on the Court's ruling in *Carpenter*, individuals now have a "*reduced* expectation of privacy in information knowingly shared with another," for historical cell-site data, anyway.[114] Despite proffering new language that

109. *Id.* ("There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today.").

110. *Id.* at 2220 (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

111. *Id.* (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979) ("[I]n no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements to third parties.")).

112. *Smith*, 442 U.S. at 750 (Marshall, J., dissenting).

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

114. *Id.* at 2219 (italics added).

suggests a revised traditional third-party doctrine, the Supreme Court emphasized that its decision does not change the holding in *Miller* and *Smith*.[115]

IV. THE DICHOTOMY BETWEEN *MILLER*/*SMITH* AND *CARPENTER* IN THE DIGITAL WORLD

"Why is cell site location information more sensitive than bank records, which particularly today, when a lot of people don't use cash much, if at all, a bank record will disclose purchases?"[116]

A. Traditional Third-Party Doctrine versus Digital Third-Party Doctrine

Prior to *Carpenter*, the Supreme Court applied the third-party doctrine in an all-or-nothing fashion. By this logic, if the third-party doctrine applied, the individual that volunteered information to a third party held no privacy interest in that information.[117] This means that under *Miller* and *Smith*, the government can request information from third parties using a subpoena instead of a warrant.[118] As explained in *Miller* and *Smith*, if an individual shares information with a third party, he lacks any reasonable expectation of privacy in that information.[119] The reason given by the Supreme Court is that individuals assume the risk that their information will be divulged to the world when shared with third parties.[120] Not only do individuals assume that risk, but individuals lack a connection to their information shared with a third

115. *Id.* at 2220 (holding that its decision "do[es] not disturb the application of *Smith* and *Miller*.").

116. Transcript of Oral Argument at 5, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402) (asked by Justice Alito).

117. United States v. Miller, 425 U.S. 435, 442–44 (1976); Smith v. Maryland, 442 U.S. 735, 743–44 (1979); Couch v. United States, 409 U.S. 322, 335–36 (1973); United States v. White, 401 U.S. 745, 751–52 (1971) (plurality opinion); Hoffa v. United States, 385 U.S. 293, 302 (1966).

118. *Miller*, 425 U.S. at 442; *Smith*, 442 U.S. at 745–46.

119. *Miller*, 425 U.S. at 443 (holding that a bank account holder has no reasonable expectation of privacy in his bank records detailing his financial activity); *Smith*, 442 U.S. at 743–44 (holding that individuals lack a reasonable expectation of privacy in the phone numbers dialed from inside the home).

120. *See, e.g.*, *Miller*, 425 U.S. at 443 (concerning financial records); *see also Smith*, 442 U.S. at 743–44 (concerning phone records); *see also White*, 401 U.S. at 751–52 (concerning personal conversations).

party because the individual can "neither [assert] ownership nor possession" in the records maintained, stored, and produced by the third party.[121]

In the digital world we live in today, *Carpenter* declined to apply the traditional third-party doctrine to historical cell-site location information.[122] If digital data is involved, an individual might have a "*reduced* expectation of privacy in information knowingly shared with another."[123] Unlike *Miller* and *Smith*, the government must generally obtain a warrant to obtain digital data, such as historical cell-site location information, from third parties.[124] Because *Carpenter* concerned digital data, namely the data generated from a cell-phone's connectivity to cell-site towers, it follows that two separate third-party doctrine theories now exist: the (1) traditional third-party doctrine governed by *Miller* and *Smith*, and the (2) digital third-party doctrine governed by *Carpenter*.[125]

Before delving into the digital third-party doctrine, it is important to understand why the Supreme Court felt it necessary to avoid using the existing traditional third-party doctrine. First, cell-site location information is qualitatively different than bank statements or phone records.[126] In other words, cell-site location information has the capability of revealing personal and intimate details that could not be compared to the revealing nature of bank records or phone records.[127] Second, cell-site location information is quantitatively different than bank statements or phone records. That is, cell-

---

121. Carpenter v. United States, 138 S. Ct. 2206, 2227 (2018) (Kennedy, J., dissenting) (citation omitted) (explaining that *Miller* and *Smith* limit an individual's ability to "assert Fourth Amendment interests in property to which they lack a 'requisite connection.'"); *Miller*, 425 U.S. at 440; *Smith*, 442 U.S. at 741.

122. *Carpenter*, 138 S. Ct. at 2216–17 (majority opinion) ("But while the third-party doctrine applies to telephone numbers and bank records, it is not clear whether its logic extends to the qualitatively different category of cell-site records.").

123. *Id.* at 2219 (italics in original).

124. *Id.* at 2221 ("Before compelling a wireless carrier to turn over a subscriber's CSLI, the Government's obligation is a familiar one—get a warrant.").

125. Change to the traditional third-party doctrine comes as no true surprise. *See, e.g.*, United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (emphasizing that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

126. *Carpenter*, 138 S. Ct. at 2209–10.

127. *Id.*

site location information paints a much broader and detailed picture about an individual than do bank records or phone records.[128] One reason for this is the sheer volume of location information that cell providers document and maintain for years.[129] Third, unlike conducting business with a bank or making a phone call, individuals do not truly share their cell-site location information to third parties.[130] The high Court reasons that cell phones are considered a necessity in the modern age, and carrying a cell phone in public is required in order to participate "in modern society."[131] Since individuals must possess (and carry) a cell phone, such logic does not extend to individuals having knowledge that their location information is being shared with wireless providers.[132] Fourth, unlike the affirmative act of dialing numbers to make a phone call or swiping a debit card to make a financial transaction, individuals do not, themselves, signal cell-site towers and have their cell-site location information documented.[133] Merely carrying a cell phone in one's pocket is all that is needed to signal a cell tower because whenever a cell phone is turned on, it automatically alerts the nearest cell tower.[134] This process enables the cell phone—and by that, the service provider—to document

128. *Id.* at 2219 ("In mechanically applying the third-party doctrine to this case, the Government fails to appreciate that there are no comparable limitations on the revealing nature of CSLI.").

129. *Id.* at 2210, 2219 (noting that a majority of wireless providers store location information for five years).

130. *Id.* at 2210, 2219–20.

131. *Id.* at 2219–20.

132. *See, e.g.*, *In re* United States for an Order Directing Provider of Elec. Commun. Serv. To Disclose Recs. to the Gov't, 620 F.3d 304, 317 (3d Cir. 2010) (explaining that "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way . . . [because] it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information.").

133. *See, e.g.*, State v. Earls, 214 N.J. 564, 577 (N.J. 2013) (noting that "[c]ell phones can be tracked when they are used to make a call, send a text message, or connect to the Internet—or when they take no action at all, so long as the phone is not turned off.").

134. *Carpenter*, 138 S. Ct. at 2220 (explaining that "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI.").

and improve connectivity of the cell phone.[135] As a result, it is the cell phone, not the user of the cell phone that takes steps to share location information.[136] For these reasons, *Carpenter* declined to extend the traditional third-party doctrine to cell-site location information.[137]

Therefore, the digital third-party doctrine requires assessment of the (1) nature of the information and (2) voluntariness. Assessing the nature of the information requires examination of how detailed, comprehensive, and intimate the information is. Accordingly, both (a) quantitative and (b) qualitative assessments of the information surveilled should be considered. Second, the Supreme Court implies that voluntariness should be assessed two-fold: by examining how necessary the device is according to the status quo, then considering whether the individual has taken any affirmative act to convey information to a third party.[138] Thus, when examining voluntariness, both the (a) pervasiveness of the device and any (b) affirmative act taken by the individual should be assessed.[139]

Going forward, courts will invariably engage in an ad-hoc factual inquiry when faced with digital data, then decide whether to apply the traditional rule represented by *Miller* and *Smith*, or the digital rule represented by *Carpenter*.[140] To what extent does *Carpenter*'s digital rule apply to other means of digital data, like a cell phone's Internet browsing history, or the

---

135. *Earls*, 214 N.J. at 576–79 (discussing the basics of how cell-site location information is generated).

136. *See In re* Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 750 (S.D. Tex. 2005) (explaining that cell phones search for signal "every seven seconds or when the signal strength weakens, regardless of whether a call is placed.").

137. *Carpenter*, 138 S. Ct. at 2209, 2216–17 (explaining that "[t]he digital data at issue—personal location information maintained by a third party—does not fit neatly under existing precedents.").

138. *See Carpenter*, 138 S. Ct. at 2220 (citation omitted) (explaining that "[i]n the first place, cell phones and the service they provide are . . . indispensable to participation to modern society." And "[s]econd, a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up.").

139. *Id.*

140. *See, e.g.*, People v. Harris, 945 N.Y.S.2d 505, 507–10 (N.Y. Crim. Ct. 2012) (holding that a Twitter user had no Fourth Amendment standing to challenge a lawful subpoena issued against the company for locational information embedded in his posts because he voluntarily shared that information with Twitter).

location information gathered by navigational apps on a cell phone?[141] Even more puzzling is that individuals still maintain no expectation of privacy in "a lifetime of bank or phone records," but do maintain some expectation of privacy in historical cell-site location information.[142] As discussed below, the Supreme Court's skewed valuation of the privacy interests maintained in digital data versus bank statements and phone records is mind-boggling.[143] Bank records, credit card records, and phone records are just as qualitatively and quantitively comparable with digital data, similar to cell-site location information. Today, as technology even allows for individuals to make purchases "[w]ith just the click of a button"[144] on their cellular device, the Court's reasoning in *Carpenter* overlooks the fact that *Miller* and *Smith* are implicated in digital data.

1. Digital Data

On March 12, 2020, the World Wide Web ("Web") turns thirty-one.[145] To some, the Web's birthday is a celebration. But to others, the Web's birthday is simply a reminder that the Web keeps tabs on its users. As former Google CEO Eric Schmidt put it: "We know where you are. We know where you've been. We can more or less know what you're thinking about."[146]

---

141. *See, e.g., Fourth Amendment & the Internet*, *supra* note 28, at 1006 (questioning "How should the Fourth Amendment apply to the Internet? What kinds of online surveillance should the Constitution permit? When should the government be allowed to monitor a criminal suspect's e-mail, web surfing, or instant messaging?").

142. *Carpenter*, 138 S. Ct. at 2267 (Gorsuch, J., dissenting) ("All we know is that historical cell-site location information (for seven days, anyway) escapes *Smith* and *Miller*'s shorn grasp, while a lifetime of bank or phone records does not.").

143. *See, e.g.*, *id.* at 2262, (questioning "Why is someone's location when using a phone so much more sensitive than who he was talking to (*Smith*) or what financial transactions he engaged in (*Miller*)? I do not know and the Court does not say.").

144. *Id.* at 2218 (majority opinion).

145. *See generally* Susannah Fox & Lee Rainie, *The Web at 25 in the U.S.*, PEW RES. CTR. (Feb. 27, 2014), https://www.pewinternet.org/2014/02/27/the-web-at-25-in-the-u-s/ [https://perma.cc/Q3PU-8ZGE].

146. Derek Thompson, *Google's CEO: 'The Laws are Written by Lobbyists,'* THE ATLANTIC (Oct. 1, 2010), https://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/ [https://perma.cc/JPC5-YZAT].

The use of the Internet has raised, and continues to raise, many privacy concerns considering the fact that the majority of Americans use the Internet.[147] In the twenty-first century: 73% of adults have used or currently use YouTube; 69% of adults have used or currently use Facebook; 37% of adults have used or currently use Instagram; 28% of adults have used or currently use Pinterest; 27% of adults have used or currently use LinkedIn; 24% of adults have used or currently use Snapchat; 22% of adults have used or currently use Twitter; 20% of adults have used or currently use WhatsApp; and 11% of adults have used or currently use Reddit.[148] Simply put, "[t]he reality of today's world is that social media, whether it be Twitter, Facebook, Pinterest, Google+ or any other site, is the way people communicate."[149]

The Internet gave rise to social media, whose devaluation of privacy has caused an irreversible outcome. Search engines like Google and Yahoo, for example, routinely gain revenue from selling user information.[150] A user's search query can include directions to a mistress' residence, symptoms of a sexually transmitted disease, or the "top 10" dating apps, just to name a few.[151] Another popular foe is Facebook. The tech giant recently found itself under scrutiny for the way it handled its 50 million users in the wake of Cambridge Analytica's access to the users' data.[152] Still, "[r]oughly two-thirds of U.S. adults (68%)" reported being Facebook users in 2018, "and

147. Monica Anderson et al., *10% of Americans Don't Use the Internet. Who Are They?*, PEW RES. CTR. (Apr. 22, 2019), https://www.pewresearch.org/fact-tank/2019/04/22/some-americans-dont-use-the-internet-who-are-they/ [https://perma.cc/XK5R-H783].

148. Andrew Perrin & Monica Anderson, *Share of U.S. Adults Using Social Media, Including Facebook, Is Mostly Unchanged Since 2018*, PEW RES. CTR. (Apr. 10, 2019), https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/ [https://perma.cc/7UNY-3X3M].

149. People v. Harris, 945 N.Y.S.2d 505, 507 n.3 (N.Y. Crim. Ct. 2012).

150. *See* Ira Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 271–72 (2008).

151. Vivian Adame, *Consumers' Obsession Becoming Retailers' Possession: The Way that Retailers are Benefiting from Consumers' Presence on Social Media*, 53 SAN DIEGO L. REV. 653, 659–60 (2016).

152. *See* Tiffany Hsu & Cecilia Kang, *Demands Grow for Facebook To Explain Its Privacy Policies*, N.Y. TIMES (Mar. 26, 2018), https://www.nytimes.com/2018/03/26/technology/ftc-facebook-investigation-cambridge-analytica.html [https://perma.cc/U7JK-3ND4].

roughly three-quarters of those users access[ed] Facebook on a daily basis."[153] Since 2018, the number of Facebook users has virtually remained the same.[154] In essence, the quantity and quality of information obtained from the use of the Internet is alarming,[155] but any eagerness of users to discontinue using data-intensive applications such as Facebook is not statistically evident.[156]

Today, more Americans either use or own a cell phone than a desktop or laptop computer.[157] The growing spread of cell phones has arguably surpassed any other form of technology.[158] Without a cell phone, it is difficult to imagine how an individual could effectively participate in modern society.[159] In fact, at least 95% of Americans own a cell phone,[160] resulting in a decline of desktop or laptop ownership.[161] In the not-too-distant future, the

153. Aaron Smith & Monica Anderson, *Social Media Use in 2018*, PEW RES. CTR. (Mar. 1, 2018), https://www.pewinternet.org/wp-content/uploads/sites/9/2018/02/PI_2018.03.01_Social-Media_FINAL.pdf [https://perma.cc/DA7S-S7K9].

154. Perrin & Anderson, *supra* note 148.

155. *See, e.g.*, Riley v. California, 573 U.S. 373, 395–96 (2014) ("An Internet search and browsing history . . . could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.").

156. Perrin & Anderson, *supra* note 148.

157. Paul Hitlin, *Internet, Social Media Use and Device Ownership in U.S. Have Plateaued After Years of Growth*, PEW RES. CTR. (Sept. 28, 2018), https://www.pewresearch.org/fact-tank/2018/09/28/internet-social-media-use-and-device-ownership-in-u-s-have-plateaued-after-years-of-growth/ [https://perma.cc/X7GX-885Y].

158. Michael DeGusta, *Are Smart Phones Spreading Faster than Any Technology in Human History?*, MIT TECH. REV. (May 9, 2012), https://www.technologyreview.com/s/427787/are-smart-phones-spreading-faster-than-any-technology-in-human-history/ [https://perma.cc/C6L9-BFH8].

159. *Riley*, 573 U.S. at 385 (noting that phones have become "such a pervasive and insistent part of daily life" that carrying one is indispensable to participation in modern society).

160. *Mobile Fact Sheet*, PEW RES. CTR. (June 12, 2019), https://www.pewinternet.org/fact-sheet/mobile/ [https://perma.cc/P5GQ-T6RL].

161. Hitlin, *supra* note 157.

number of cell phone ownership is expected to reach north of 270 million.[162] This is hardly surprising considering that cell phones are much cheaper, easier to carry, and can be used in more locations than a desktop or laptop computer can be used.[163] Cell phones could also be called "minicomputers"[164] because of their limitless capabilities: A cell phone can act as a telephone, camera, video player, diary, calendar, television, map, newspaper, video game, photo album, stereo, and more.[165] Aside from these basic functions—most of which already equipped into cell phones—a cell phone user also has the option of downloading applications, otherwise known as "apps."

With the use of apps, digital connectivity has made it possible to perhaps *never* have to leave your home. Tired of being single? Download a dating app.[166] Over 15% of U.S. adults have spiced things up digitally.[167] Tired of going to the grocery store? Amazon has got you covered.[168] Need to make some extra cash to pay rent? Apps exist for you to make money while lounging on your living room love seat.[169] Hungry? There's an app

---

162. *Research Peek of the Week: Smartphone Users in the US Expected to Reach Over 270 Million by 2022,* INTERNET INNOVATION ALLIANCE (July 3, 2018), https://internetinnovation.org/general/research-peek-of-the-week-smartphone-users-in-the-us-expected-to-reach-over-270-million-by-2020/ [https://perma.cc/E3N5-2TMF].

163. *See, e.g.*, *Riley*, 573 U.S. at 394–96 ("Even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on.").

164. *Id.* at 393.

165. *See, e.g.*, *id.* (explaining that cell phones can "easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.").

166. Mark Jansen, *The Best Dating Apps for 2019*, DIGITAL TRENDS (Aug. 17, 2019, 12:30 PM), https://www.digitaltrends.com/mobile/best-dating-apps/ [https://perma.cc/4NFZ-CGCT].

167. Aaron Smith, *15% of American Adults Have Used Online Dating Sites or Mobile Dating Apps*, PEW RES. CTR. (Feb. 11, 2016), https://www.pewinternet.org/2016/02/11/15-percent-of-american-adults-have-used-online-dating-sites-or-mobile-dating-apps/ [https://perma.cc/JZF2-GCZJ].

168. *See, e.g.*, Deborah Weinswig, *Online Grocery Set To Boom In 2018 (As Amazon Acknowledges Online Grocery A Tough Market To Crack)*, FORBES (Mar. 1, 2018, 4:10 PM), https://www.forbes.com/sites/deborahweinswig/2018/03/01/online-grocery-set-to-boom-in-2018-as-amazon-acknowledges-online-grocery-a-tough-market-to-crack/#e406fba520b9 [https://perma.cc/URC5-L4VT].

169. *17 Great Apps That Will Pay You Money in 2019*, THE WORK AT HOME WIFE (Aug. 25, 2019), https://theworkathomewife.com/apps-will-pay-money/ [https://perma.cc/F6TZ-VK6A].

for that too.[170] Need alcohol to celebrate a forgotten birthday? Download an app.[171] Are you a Cannabis user or supporter? There's an app to connect you with other Cannabis users or supporters.[172] Medical apps also exist to monitor and support one's health, such as assisting recovering alcoholics.[173] Unsurprisingly, the average number of apps Americans use daily is nine, while the monthly average is thirty.[174]

Is using a navigation app to prevent getting lost worth giving up your exact location? Waze might certainly think so.[175] The GPS navigation app, purchased by Google for a billion dollars,[176] not only has the ability to detect automobile accidents and faster routes, but can also detect law enforcement.[177] Yet, detecting law enforcement is less surprising than Waze's ability to promote local eateries when a vehicle is at a standstill, otherwise

---

170. *See, e.g.*, Alina Bradford & Gia Liu, *The Best Food Delivery Apps of 2019*, DIGITAL TRENDS (July 30, 2019, 2:37 PM), https://www.digitaltrends.com/home/best-food-delivery-apps/ [https://perma.cc/MBC7-6R8D].

171. *See, e.g.*, Danielle St. Pierre, *Never Run Out of Boose Again Thanks to These 7 Alcohol-Delivery Apps*, BEST (Jan. 2, 2019), https://www.bestproducts.com/eats/g1616/liquor-alcohol-delivery-apps/ [https://perma.cc/NQY7-9CCN].

172. *See, e.g.*, *The Biggest Cannabis Social Media Community!*, PUFFY, https://puffyapp.com [https://perma.cc/4VXX-CVDE] ("Puffy App is a mobile platform for users to puff, connect, and meet up with new friends.").

173. *See, e.g.*, Jessica Timmons, *The Best Alcohol Addiction Recovery Apps of 2019*, HEALTHLINE (Apr. 24, 2019), https://www.healthline.com/health/addiction/top-alcoholism-iphone-android-apps#twenty—four-hours-a-day [https://perma.cc/LY7N-3JML].

174. Sarah Perez, *Report: Smartphone Owners Are Using 9 Apps per Day, 30 per Month*, TECHCRUNCH (May 4, 2017), https://techcrunch.com/2017/05/04/report-smartphone-owners-are-using-9-apps-per-day-30-per-month/ [https://perma.cc/GZN5-DHNK].

175. *Wazeopedia*, WAZE, https://wazeopedia.waze.com/wiki/USA/About [https://perma.cc/D6CU-WZNK] ("Waze is a 100% free turn-by-turn GPS navigation application that provides real-time traffic updates.").

176. Ingrid Lunden, *Google Bought Waze For $1.1B, Giving A Social Data Boost To Its Mapping Business*, TECHCRUNCH (June 11, 2013, 8:37 AM), https://techcrunch.com/2013/06/11/its-official-google-buys-waze-giving-a-social-data-boost-to-its-location-and-mapping-business/ [https://perma.cc/F3Y7-AM7Y].

177. *About Us*, WAZE (Sept. 16, 2019), https://www.waze.com/about [https://perma.cc/A2TY-CXKV].

known as a "zero-speed takeover."[178] Ever wonder why an ad surfaces your Waze screen when you are at a stop sign or stopped in traffic? This is because "Google isn't just monitoring what you do online; it's watching you while you're in your car, too."[179] For some, navigation is a necessity—and to limit being late to work or getting lost, the navigation app has clear benefits. But to others, GPS-gathered data is alarming because of the wealth of personal information that can be revealed, like "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."[180] Despite Waze having the ability to "ping[] its users' GPS every second and store[] that data, sometimes sharing it with local governments,"[181] cell phone users nonetheless continue to use the app.

The bottom line is that using technology has the potential to create a permanent digital trail. This digital trail can reveal both personal and mundane information about one's identity. So where does the Fourth Amendment come into play? Under the traditional third-party doctrine, *Miller* and *Smith* imply that law enforcement can obtain, for example, DNA information from Ancestry.com or 23andMe with a subpoena instead of a warrant supported by probable cause.[182] But under the digital third-party doctrine, the only category *Carpenter* adds protection to is historical cell-site location information.[183] This category excludes Facebook messages, information from

---

178. Greg Sterling, *Waze Conquers 'Digital Dark Zone' with in-car, out-of-home ad Coordination,* SEARCH ENGINE LAND (Mar. 18, 2019, 10:24 AM), https://searchengineland.com/waze-conquers-digital-dark-zone-with-in-car-out-of-home-ad-coordination-314111/ [https://perma.cc/EF3W-2BCE].

179. Monica Burton, *Waze is Watching You and It Knows You Want McRibs*, EATER (Mar. 19, 2019, 2:28 PM), https://www.eater.com/2019/3/19/18272694/waze-app-ads-steer-drivers-to-mcdonalds-mcribs/ [https://perma.cc/32X8-T5C4].

180. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (quoting People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009); *see also* Michael Mattioli, *Article: Autonomy in the Age of Autonomous Vehicles*, 24 B.U. J. SCI. & TECH. L. 277, 293 (2018).

181. Burton, *supra* note 179.

182. Carpenter v. United States, 138 S. Ct. 2206, 2262–63 (2018) (Gorsuch, J., dissenting) (answering that "*Smith* and *Miller* say yes" to law enforcement being able to obtain "DNA from 23andMe without a warrant or probable cause.").

183. *See id.* at 2221 (majority opinion) (holding that "an order issued under Section 2703(d) of the Act is not a permissible mechanism for accessing historical cell-site records.").

the Cannabis app, the dating app, bank and phone records, and other digital data. The Supreme Court informs us that only cell-site location information is deserving of some expectation of privacy because this information somehow reveals more personal information about an individual than other data.[184] It remains unexplained why an individual's location information is more intimate than the troves of bank records or credit card records revealing, by date and time, a virtual biography of an individual.[185]

2. Physical Information Turns Digital

Today's Supreme Court discounts the fact that physical data, like a debit card or credit card, is comparable to cell-site location information.[186] Concededly, debit cards and credit cards do not ping to nearby cell towers, nor do these cards have a tracking chip (to date) that reveals the location information of the card.[187] However, statements generated by a debit card or credit card yield similar to identical information as cell-site location information. First, debit cards and credit cards can produce information with the same level of accuracy as cell-site location information. Second, financial statements are far more revealing than the mere vicinity in which a cell phone is located. And third, with the digitalization of bank cards and credit cards, law enforcement can learn about the identity of an individual without the individual even leaving his or her home.

The precision of bank records far exceeds that of CSLI. To illustrate this, suppose Jeff visits a shopping center for seven days straight and keeps his cell phone on him at all times. Further suppose that Jeff makes some type of purchase at the shopping mall for each day he is there. He uses his banking card because he never carries cash on him. Using only CSLI and banking records, which data provides law enforcement with the most actionable in-

184. *Id.* at 2216–17.

185. *See id.* at 2262 (Gorsuch, J., dissenting) (questioning "Why is someone's location when using a phone so much more sensitive than who he was talking to (*Smith*) or what financial transactions he engaged in (*Miller*)? I do not know and the Court does not say.").

186. *See id.* at 2219 (majority opinion) ("In mechanically applying the third-party doctrine to this case, the Government fails to appreciate that there are no comparable limitations on the revealing nature of CSLI.").

187. *See, e.g.*, Tylene Welch, *Can You Track a Debit Card or Credit Card with a Smart Chip?*, FISCAL TIGER (Feb. 28, 2019), https://www.fiscaltiger.com/can-track-debit-card-credit-card-smart-chip/ [https://perma.cc/B5YV-H8N6].

formation? Beginning with CSLI, obtaining CSLI will provide law enforcement insight as to the vicinity that Jeff was physically located based on his cell phone pinging to the cell towers. This, of course, assumes that a cell tower is located near the shopping center. Intelligent as law enforcement officials are, they may be able to deduce that Jeff was at the shopping mall each day based on the fact that Jeff—that is, his cell phone—triggered a cell site next to the shopping mall each day he was there. But if law enforcement wanted to obtain the cell-site location information for the past seven days, they would need to obtain a warrant.[188] *Carpenter* makes that clear.[189]

On the other hand, if law enforcement officials obtained Jeff's banking records, to reiterate the late Justice Brennan's position, the seven-day banking records would "provide[] a virtual current biography."[190] Jeff's banking records would reveal (1) what Jeff purchased, (2) the specific store Jeff made the purchase at, (3) the location of the store Jeff made the purchase at, (4) the amount Jeff spent on each purchase, and (5) the date and time of each purchase Jeff made. But unlike CSLI, law enforcement can obtain this information through compulsory means—*i.e.*, by subpoenaing the bank for Jeff's transaction history for the past seven days. Taking a step further, while banking records can also reveal the flowers or jewelry Jeff purchased for his mistress, the $199 handgun suspected of criminal wrongdoing, the adult store video, and more, CSLI could not provide that information. Instead, CSLI would only reveal the vicinity of Jeff's physical whereabouts,[191] or the vicinity of a cell phone lent to a family member or friend, left in a taxi, or stolen.[192]

---

188. *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.").

189. *Id.* at 2221.

190. United States v. Miller, 425 U.S. 435, 451 (1976) (Brennan, J., dissenting).

191. *See Carpenter*, 138 S. Ct. at 2217 (emphasizing that the cell-site location information merely revealed "that Carpenter's cell phone was in the general vicinity of four of the nine robberies.").

192. Although not explored, there may be situations where only one or two stores are near a cell tower, and by process of elimination, law enforcement could accurately identify where an individual was.

Second, while cell-site location information can create a chronological timeline of an individual's past and present,[193] "the totality of bank records provides a virtual current biography"[194] of a person's past, present, *and* future. With bank records in hand, the government can learn and deduce highly personal details.[195] For example, banking records allow the government to: (1) catalogue an individual's expenses and approximate his or her income based on deposits; (2) determine where and what an individual eats for breakfast, lunch, and dinner; (3) determine who an individual's doctor is and when he or she visited the hospital; (4) determine the political preference or porn magazine an individual is subscribed to; (5) determine whether an individual is a heavy drinker based on frequent trips to the liquor store or bar receipts; (6) determine where an individual takes his family or mistress on vacation; (7) determine the exact date and time an individual grocery shops at Whole Foods; (8) determine whether an individual poorly manages his money; (9) determine an individual's rent amount, cost of utilities, and other household expenses; and (10) determine the ATM withdrawal at the sole ATM machine inside a brothel.

With this information, the government can ascertain an individual's habits, hobbies, health, political preference, morals, and much more. Indeed, where bank records and credit card records are distinguished from cell-site location information is the fact that the government can study and predict an individual's future conduct. For example, past financial statements could help estimate the cost of next month's rent, utilities, child support, or even which bar the individual will be at next Friday since that individual's past financial statements reveal a trend. These very few—and realistic—examples help shed light on the fact that financial statements provide law enforcement with a time machine capable of traveling both in the past and in the

193. *Carpenter*, 138 S. Ct. at 2210 (CSLI "give[s] the Government near perfect surveillance and allow it to travel back in time to retrace a person's whereabouts.").

194. *Miller*, 425 U.S. at 451 (Brennan, J., dissenting).

195. *See id.*; *see also* Transcript of Oral Argument at 6, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402) (Justice Kennedy reasoned that bank records differ from cell-site location information "[p]articularly because the information in the bank records that Justice Alito referred to are not publicly known. Your whereabouts are publicly known. People can see you. Surveillance officers can follow you. It seems to me that this is much less private than - than the case that Justice Alito is discussing.").

future. And unlike the five-year retention of cell-site location information,[196] a majority of larger banks maintain records for seven years.[197]

Third, the digitalization of debit cards and credit cards makes financial statements much more revealing in today's market. Although credit cards and debit cards are physical in form, they can indeed be digitized. Many platforms, including Apple and Samsung, have built into their cellular devices a "digital wallet."[198] Apple in particular has advertised that its "Apple Pay" digital tool "is even simpler than using your physical [debit or credit] card, and safer too."[199] With the digitalization of debit cards and credit cards, law enforcement can learn about an individual as if the individual live-streamed his activity within his home.[200] The same could not be said for cell-site location information. Without a cell phone or cell tower, cell-site location information is not generated. Yet, with a cell phone's ability to store a virtual bank, information about the user can be generated while in public and in the privacy of the user's home. Indeed, virtual banking has made it possible to conduct business with vendors without having to leave home.[201] The Supreme Court insists that a cell phone has the capability of revealing the "sum of an individual's private life," which is far more than what is "tucked into a wallet."[202] But to carry a cell phone today is to carry a virtual bank.

---

196. *Carpenter*, 138 S. Ct. at 2218 (emphasizing that a majority of wireless providers store location information for five years).

197. *See, e.g.*, *Paperless Statements*, CHASE, *https://www.chase.com/personal/mobile-online-banking/login-paperless/paperless-faqs* [https://perma.cc/H9QS-BKE2] (explaining that "you can securely access up to 7 years of statements online.").

198. Mark Edwin Burge, *Apple Pay, Bitcoin, and Consumers: The ABCs of Future Public Payments Law*, 67 HASTINGS L.J. 1493, 1523–24 (2016).

199. *Secure, Simple, and Even More Useful*, APPLE, http://www.apple.com/apple-pay [*https://perma.cc/C3CA-PFPW*] (describing the usage of Apple's Wallet app).

200. *See* Note, *If These Walls Could Talk: The Smart Home And The Fourth Amendment Limits of The Third Party Doctrine*, 130 HARV. L. REV. 1924, 1933 (2017) (explaining that technology presents the risk of people "inviting the government into their homes and giving it a front-row seat to their most intimate conversations.").

201. One example is food delivery services like Uber Eats. *See, e.g.*, *How Uber Eats Works*, UBER EATS, https://about.ubereats.com/en/ [https://perma.cc/Z28L-JVJY] (explaining how Uber Eats works).

202. Riley v. California, 573 U.S. 373, 394–95 (2014) ("The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet.").

To that end, it seems clear that what an individual purchases on his or her cell phone is far more revealing than location information. With the latter, law enforcement must infer, based on only having information pin-pointing that an individual was in a certain area, that the individual was indeed at the particular place. But with the former, not only can law enforcement obtain information concerning the cost and type of item purchased, but also where that item was purchased from and delivered to, giving law enforcement the full picture.

B. The Third-Party Doctrine Is "[I]ll [S]uited,"[203] Period.

Carpenter explains that the third-party doctrine is "ill suited to the digital age."[204] Even if this were true, it was no less true in *Miller* and *Smith*. *Miller* and *Smith* teach us that individuals have no expectation of privacy in their banking activity and the phone numbers dialed on a phone.[205] Apparently, because these records are "possessed, owned, and controlled" by a third party, society has no choice but to assume that the third party may display the collected information for the world to see, including the world of law enforcement.[206] But does society truly expect that their finances and family calls will be broadcast to the world?[207] Surely "no one believes that, if they ever did."[208] The majority in *Carpenter* supports its position by informing us that individuals have no choice but to keep a phone on their persons when in public, leading us to assume that individuals could not possibly

---

203. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

204. *Id.*

205. United States v. Miller, 425 U.S. 435, 442–43 (1976) (holding that a bank account holder has no reasonable expectation of privacy in his bank records detailing his financial activity); Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (holding that individuals lack a reasonable expectation of privacy in the phone numbers dialed from inside the home).

206. *See* Carpenter v. United States, 138 S. Ct. 2206, 2226–27 (2018) (Kennedy, J., dissenting). *But see In re* United States *ex rel.* Hist. Cell Site Data, 747 F. Supp. 2d 827, 845 (S.D. Tex. 2010) ("[C]onsumers are not forced to sacrifice locational privacy as the price of using cell phones.").

207. *See, e.g.*, Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 VAND. L. REV. 1289, 1315 (1981) ("It would be unreasonable to assume that the defendant in Katz would have had less of an expectation of privacy in the numbers he dialed from his own private telephone than he did in the content of a conversation in a public telephone booth.").

208. *Carpenter*, 138 S. Ct. at 2262 (Gorsuch, J., dissenting).

volunteer their information to third parties based on the necessity of having a cell phone.[209] But what about the necessity of using banking services? Does the fact that individuals constantly share their location information on social media platforms affect the Court's opinion?[210]

If having a cell phone is necessary to participate in this day-and-age, it is equally as "impossible to participate in the economic life of contemporary society without maintaining a bank account," said Justice Brennan over forty years ago.[211] Fast-forward forty years, does the Court expect for society to maintain a home banking service?[212] Rather than store and protect troves of financial records that "reveal much about a person's activities, associations, and beliefs,"[213] society instead chooses to entrust that information with a bank.

> [T]he disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account. In the course of such dealings, a depositor reveals many aspects of his personal affairs, opinions, habits and associations.[214]

When a burglar enters a home, the burglar's likely target is the safe kept in the basement, not the bedsheets. Inside the safe can include cash, checks, passports, social security cards, birth certificates, personal finance records, and more. But when a burglar enters a bank, the likelihood of the burglar requesting cash, financial statements, and all other personal documents of only John Doe is slim to nil. The need to use conventional banking

---

209. *Id.* at 2220 (majority opinion).

210. *See generally* Rachel Levinson-Waldman, *Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media*, 71 OKLA. L. REV. 997 (2019) (exploring the privacy implications of social media use).

211. United States v. Miller, 425 U.S. 435, 451 (1976) (Brennan, J., dissenting).

212. *See* Ashdown, *supra* note 207, at 1313–14. (explaining that "it cannot be said that financial disclosures to a bank are truly voluntary, since it is a virtual necessity to maintain a bank account in order to participate economically in contemporary society.").

213. *Miller*, 425 U.S. at 453 (Brennan, J., dissenting).

214. *Id.* at 451.

methods is especially true when mom and dad want to keep a separate college account for their child. Entrusting hundreds of thousands of dollars to a safe accessible by, for example, guessing a pin number, is unnecessarily risky. That risk does not fully escape in the hands of the bank, but the safety measures undertaken by a bank adds more comfort than constantly thinking about the $200,000 in the home safe. Using a conventional bank is simply a necessity worth acknowledging under the Fourth Amendment's expectations of privacy analysis.

It bears repeating that the third-party doctrine is "ill suited,"[215] period. Under the Court's assessment of the third-party doctrine, since society lacks true knowledge that its location information is being received and stored by a third party, society does not genuinely volunteer that information to the wireless provider as a new customer does to the teller at a bank.[216] The Court reasons that a cell phone automatically triggers cell towers without much, if any, assistance from the carrier of the cell phone.[217] But it is the carrier of the cell phone that takes the affirmative act of stepping outside their home and entering the public.[218] But for the user of the cell phone, the cell phone presumably would not trigger cell-site towers.[219] It would seem that whatever affirmative act the Court expects individuals to take must be a reasonable one. After all, the Court dismissed the option of individuals removing the battery from their cell phone before entering the public to avoid leaving behind a digital trail.[220] Still, it remains unexplained what would happen if society learned that its location information is being recorded and maintained by wireless providers? Justice Alito asked this very question: "[W]hat will

---

215. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

216. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

217. *Id.*

218. *See, e.g.*, United States v. Graham, 824 F.3d 421, 429–30 (4th Cir. 2016) (explaining that "[w]ith respect to the nature of CSLI, there can be little question that cell phone users 'convey' CSLI to their service providers. After all, if they do not, then who does?").

219. Understandably, the possibility of cell-site towers being placed within close proximity to residential areas exists. This lends support to the Supreme Court's rationale that society members could be within their own home and still generate location information because of their cell phone's close proximity to nearby cell-site towers.

220. *Carpenter*, 138 S. Ct. at 2220 (explaining that "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume[ ] the risk' of turning over a comprehensive dossier of his physical movements.").

happen in the future if people – everybody begins to realize that this is – this is provided? If you have enough police TV shows where this is shown, then everybody will know about it, just like they know about CSI information."[221] Would individuals still have *some* expectation of privacy despite having full knowledge that their location information is being recorded and stored?[222] Answering Justice Alito's question only further contradicts the third-party doctrine.

Just as the Supreme Court instructed of the third-party doctrine in *Miller*, it should overrule its faulty application.[223] Society expects that a privacy interest attaches to bank records and phone records. While the Court protects historical cell-site location information that is observable by the naked eye, it remains unclear why financial records stored on an app (or at a conventional bank) and hidden from the naked eye are less deserving of Fourth Amendment protection. Adopting a digital third-party doctrine will not resolve the tension between the Fourth Amendment and technology, as it is a direct departure from traditional expectations and proves unworkable. What will prove workable, however, is adhering to the common understanding that what enters the public—either through physical or digital information—remains public knowledge, and that which is public knowledge does not amount to a reasonable expectation of privacy.

221. Transcript of Oral Argument at 17, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402).

222. One solution to potentially resolving the uncertainties of the third-party doctrine is to ask whether individuals have consented for third parties to share their information. *Third-Party Doctrine*, *supra* note 32, at 588–90 (arguing that "the third-party doctrine is better understood as a form of consent rather than as an application of *Katz*. Third-party disclosure eliminates privacy because the target voluntarily consents to the disclosure, not because the target's use of a third party waives a reasonable expectation of privacy.").

223. *See generally* 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/7MJ2-J2VU] (explaining that the continued use of the third-party doctrine will cause the Fourth Amendment to "become increasingly obsolete.").

V. WHAT ENTERS THE PUBLIC EYE REMAINS PUBLIC KNOWLEDGE: "THE SUM OF AN INFINITE NUMBER OF ZERO-VALUE PARTS IS ALSO ZERO."[224]

The majority in *Carpenter* begins its quest to defend against law enforcement's warrantless collection of historical cell-site location information by reiterating that, "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[225] *Carpenter* furthers its position by underscoring that "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere."[226] At the same time, the Supreme Court in *Katz* emphasized that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[227] For this reason, the reasonable expectation of privacy as to the visual observation of a person in public, as concluded in *Katz v. United States*, is zero.[228] The reasonable expectation of privacy as to a person purchasing adult magazines in an adult bookstore is, as concluded in *Maryland v. Macon*, zero.[229] The reasonable expectation of privacy as to a person's movements on the highway is, as concluded in *Knotts v. United States*, zero.[230] The reasonable expectation of privacy as to the aerial observation of a person's property is, as concluded in *California v. Ciraolo* and *Florida v. Riley*, zero.[231] In each case, the Supreme Court spoke to the privacy interests that attached to areas observable by the "intruding

224. United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010) (Sentelle, C.J., dissenting) (noting that "[t]he reasonable expectation of privacy as to a person's movements on the highway is . . . zero," and "the sum of an infinite number of zero-value parts is also zero.").

225. *Carpenter*, 138 S. Ct. at 2217 (quoting Katz v. United States, 389 U.S. 347, 351–52 (1967)).

226. *Id.*

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

228. *Id.*

229. Maryland v. Macon, 472 U.S. 463, 469 (1985).

230. United States v. Knotts, 460 U.S. 276, 281 (1983).

231. California v. Ciraolo, 476 U.S. 207, 213–14 (1986); Florida v. Riley, 488 U.S. 445, 449–50 (1989).

eye." [232] If *Katz* remains good law, and there is no indication to think otherwise, then Carpenter's public location information could not have amounted to a reasonable expectation of privacy because Carpenter was publicly exposed to nothing more than "intruding eye[s]."[233] Instead of adhering to the plain language of *Katz*, the majority in *Carpenter* supports its position by revisiting two cases it decided over a decade after *Katz*.

The first case is *United States v. Knotts*.[234] In *Knotts*, law enforcement placed a radio transmitter inside a container that was sold to the suspect and placed inside the vehicle driven by the suspect.[235] Law enforcement followed the vehicle on public streets and on the highway.[236] At some point, law enforcement lost visual observation of the moving vehicle containing the transmitter.[237] But with the aid of a helicopter that picked up the transmitter's signal, law enforcement found the location of the transmitter inside a cabin.[238] The Court concluded that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[239] The Court explained that when the suspect traveled on public streets and highways, "he voluntarily conveyed to anyone who wanted to look the fact that he was traveling" from one destination to another.[240] Additionally, despite law enforcement losing visual surveillance of the vehicle, leaving technology as the only means of discovering the suspect's final destination, "scientific enhancement of this sort raises no constitutional issues which visual surveillance would not also

232. *Katz*, 389 U.S. at 352.

233. *Id.*

234. *Knotts*, 460 U.S. 276.

235. *Id.* at 277–78.

236. *Id.* at 281.

237. *Id.* at 278.

238. *Id.* at 278–79.

239. *Id.* at 281.

240. *Id.* at 281–82.

raise."[241] Law enforcement merely identified what they would have identified had they not temporarily lost visual contact with the vehicle.[242] Accordingly, the Court held that an expectation of privacy did not extend to the visual observation of the suspect's travels in public.[243] Left responding to the possibility that individuals could be subject to "twenty-four hour surveillance" by law enforcement, the Court noted that "if such dragnet-type law enforcement practices" occur, a different ruling may give way.[244] Three decades after *Knotts*, the Court revisited the possibility of a "dragnet-type" surveillance using GPS tracking devices in *United States v. Jones*.[245]

In *United States v. Jones*, the Supreme Court similarly considered the constitutionality of tracking a vehicle's public movements with the use of technology.[246] Unlike the technological use of a beeper concealed in a container and sold to the suspect in *Knotts*, law enforcement in *Jones* physically installed a GPS tracking device underneath the suspect's vehicle.[247] The Court found that the installation of the tracking device, for the purpose of obtaining information, constituted a trespassory search under the Fourth Amendment.[248] Although law enforcement violated the Fourth Amendment, the majority stressed that it did not violate Jones's reasonable expectation of privacy under existing law.[249] This is because the "mere observation" of a vehicle traveling in public does not amount to a reasonable expectation of

241. *Id.* at 285 (noting that the radio transmitter was not used "in any way that would not have been visible to the naked eye from outside the cabin.").

242. *Id.* (explaining that "[a] police car following . . . [the suspect] at a distance throughout his journey could have observed him leaving the public highway and arriving at the cabin" with the transmitter still in the vehicle).

243. *Id.* at 281–82.

244. *Id.* at 283–84. (citation omitted).

245. United States v. Jones, 565 U.S. 400, 408–09 (2012).

246. *Id.* at 402.

247. *Id.* at 402–03.

248. *Id.* at 404.

249. *Id.* at 408–09 (noting that "the Katz reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.").

privacy since that location information is observable by the "public eye."[250] The concurring justices, however, emphasized that irrespective of "the presence or absence of a physical intrusion," a *Katz* analysis may be warranted.[251] One reason for this additional analysis is that the length of law enforcement surveillance could violate the reasonable privacy expectations that individuals expect in public.[252] Justice Alito expressed that "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable," but goes on to say that "the line was surely crossed" when that monitoring continued for four weeks.[253] On a similar point, Justice Sotomayor questioned whether society "expect[s] that their movements will be recorded and aggregated in a manner that enables the government" to collect personal information.[254] Justice Sotomayor also expressed concern towards the means of law enforcement surveillance.[255] Specifically, the use of technology versus conventional surveillance, like physically following a vehicle or viewing footage from a nearby camera poll.[256] Not only is technology cheaper than conventional techniques,[257] but when the government employs technology to surveil individuals, the subject of the surveillance likely does not know he is being monitored.[258] The odds of a suspect catching wind of having a tail by an interviewed witness or the distinct unmarked vehicle in the rear-view mirror is greater than if law enforcement employed technology.

---

250. *Id.* at 411–12 (citation omitted) (explaining that "[t]his Court has to date not deviated from the understanding that mere visual observation does not constitute a search.").

251. *Id.* at 414–18 (Sotomayor, J., concurring); *id.* at 422–23 (Alito, J., concurring in judgement).

252. *See, e.g.*, *id.* at 409 (majority opinion); *id.* at 424–25 (Alito, J., concurring in judgment).

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

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

255. *Id.* at 415–16.

256. *Id.*

257. *Id.* at 429–30 (Alito, concurring in judgment) (explaining that conventional circumstances may require "a large team of agents, multiple vehicles, and perhaps aerial surveillance," whereas "monitoring [an individual using technology is] relatively easy and cheap.").

258. *Id.* at 415–16 (Sotomayor, J., concurring).

Writing for the majority in *Jones*, Justice Scalia recognized the foreseeable problems attached to differentiating between long-term and short-term surveillance: "[I]t remains unexplained why a 4-week investigation is 'surely' too long . . . . What of a 2-day monitoring of a suspected purveyor of stolen electronics? Or of a 6-month monitoring of a suspected terrorist?"[259] The majority in *Jones* declined to use *Katz*' reasonable expectations of privacy test, and instead stressed that it would be "particularly vexing" to determine that the amount of days, weeks, months, or even years of public observation is either too long or short, especially when considering "such surveillance is constitutionally permissible."[260]

A. Assessing the Length of Surveillance Cannot Survive Under a Practical Application

It is entirely unclear what the implications would be of a Fourth Amendment that protects cumulative data collected by law enforcement. The Supreme Court explains that longer periods of police surveillance reveal information that, taken together, creates a revealing image of an individual, otherwise known as a "mosaic."[261] But this proposition is nothing more than "extravagant generalizations," which the same Court has "never held that potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment."[262] By this logic, any length of surveillance by law enforcement could run afoul of the Fourth Amendment based solely on the amount of information collected. The Supreme Court assumes that the compilation of information logically amounts to a wealth of private information.

Distinguishing between long-term and short-term surveillances takes for granted many things. The first is that *only* long-term surveillances reveal (1) quantitatively more information and (2) qualitative information. Even a single day of surveillance can reveal more about an individual than a week-long surveillance, which proves that no amount of days of surveillance auto-

259. *Id.* at 412–13 (majority opinion) (citation omitted).

260. *Id.*

261. *See id.* at 416 (Sotomayor, J., concurring) (asking "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.").

262. Dow Chem. Co. v. United States, 476 U.S. 227, 238 n.5 (1986).

matically produces a revealing "mosaic." Second, police might obtain actionable information of an individual on day ten of their surveillance, while observing little to no information on the first nine days. Third, the Court confuses possibility with certainty. Surveilling an individual for ten days could reveal nothing more than where the individual eats, which hardly amounts to a revealing "mosaic" envisioned by the Court. Fourth, law enforcement is not equipped with a crystal ball informing them as to when their collection of information implicates the Fourth Amendment. Fifth, how much information actually creates a "mosaic"? Under the mosaic theory, the collection of information would inevitably turn into a Fourth Amendment search at some undefined point, making the mosaic theory's application impracticable.[263]

A simple example might help bring some of these points to life. Suppose law enforcement monitored an individual for ten days. In those ten days, law enforcement employs physical surveillance, directing undercover officers to follow the individual each time he travels in public. Of the ten days, the individual leaves his residence and enters the public on three separate days. Of the three days the individual was in public, he was alone. The individual went to his local gym, a local restaurant, and a local grocery store. Finally, after ten days, law enforcement has uncovered: where the individual exercises, including the name of the gym and perhaps the various exercises the individual does; where the individual likes to eat, including the name of the restaurant and type of food the individual eats; and where the individual shops for groceries, including the name of the grocery store and the various groceries purchased. Now to rewind. Assume now law enforcement conduct a three-day surveillance. The individual leaves his house twice, again alone, and enters the public sphere. On the first day, the individual drives to another residence that law enforcement identified as the home of the individual's parents. The individual picks up his parents and takes them to a local mosque to pray. On the second day, the individual goes shopping at a nearby shopping mall, only this time the individual is with his significant other. After shopping, undercover officers observe three different shopping bags that the individual carried: one from Victoria's Secret; another from Rifles & Ammunition; and the third bag from Kids-R-Us.

Between the former and latter suspect, law enforcement undoubtedly uncovered more about the latter suspect who was monitored for only three days, as opposed to the former suspect who was monitored for ten days. This

263. Kerr, *supra* note 68, at 330–33 (explaining the uncertainty created under the mosaic theory as to when in the course of a surveillance a search occurs).

is but one example demonstrating the impracticability of assessing the length of law enforcement surveillance to conclude that a "mosaic" is consequently revealed. The mosaic theory can best be understood as a puzzle piece. Tasked with piecing together a disassembled 500-piece puzzle without knowing that the puzzle collectively forms the image of a colored black hole, it could take days, weeks, or months to uncover that the image is actually of a black hole. But it is the process of individually piecing together the puzzle that an individual learns of the shape, color, and measurements of the colored black hole. The collection of this information reveals more about the black hole image than does when the individual obtained the dissembled puzzle piece. At the outset, an individual may have deduced that the puzzle includes a distinct violet color, but it is through the continuous piecing together that the individual collects more information about the black hole, a revealing mosaic.

Returning back to law enforcement surveillance, one problem with the Court's adoption of the "mosaic theory" is that there is simply no practical way of measuring how much information becomes too much information, and just how long of a surveillance reveals too much information.[264] The answer, unfortunately, is not located in a dusty textbook or in a Supreme Court opinion. One reason for this absence, perhaps, is because there is no clear answer. How long law enforcement conducts surveillance is not determinative of how much information law enforcement collects. Likewise, how much information law enforcement collects is not determinative of how long law enforcement conducts surveillance. To continue assessing the length of surveillance is to contribute to the unworkable mosaic theory that should be overruled once and for all. With the inclusion of the length of government surveillance into the Fourth Amendment, law enforcement could run afoul of the Fourth Amendment even when they use ordinary investigatory techniques, such as using physical surveillance for a short period of time on individuals in public, or collecting footage from a nearby camera poll.

B. Assessing the Length of Surveillance is Incompatible with Katz

It is unclear how *Katz* could continue to survive when the length of public observation is now factored into the expectations of privacy test. The majority in *Carpenter*, while incorporating the concurring opinion in *Jones*, emphasized that the length of government surveillance, "regardless whether

264. *When Does a Carpenter Search Start—and When Does It Stop?*, *supra* note 72.

those movements were disclosed to the public at large,"[265] matters in the context of what privacy rights society expects to maintain in public. If physically surveilling a suspect in public can implicate the Fourth Amendment, what is left of the public exposure doctrine?[266] A retreat from the public exposure doctrine is a direct retreat from *Katz* itself, for the simple reason that *Katz* already decided the privacy concerns of individuals that inject themselves in the public eye. Short of explicitly mentioning "public exposure doctrine," the doctrinal rule was implicit in *Katz*' expectations of privacy test.[267] What Katz "sought to exclude when he entered the booth was not the *intruding eye*—it was the *uninvited ear*."[268] Therefore, *Katz* does not protect against the visual observations in public, so "[i]f there is no reasonable expectation of privacy in a specific public movement, how can there be any such expectation in a collection of these movements?"[269]

With respect to observing what was *once* public knowledge, as in *Carpenter*, *Katz*' application does not change. What once entered the public eye remains public knowledge. The question, then, is whether the public exposure doctrine applies only to contemporaneous observations or to past and present observations. One scholar is convinced that the public exposure doctrine is limited to contemporaneous monitoring "at that time" the individual was in public.[270] Because past movements are not "susceptible to visual surveillance," law enforcement could not use the public exposure doctrine with retroactive force.[271] Another scholar insists that the collection of historical

---

265. Carpenter v. United States, 138 S. Ct. 2206, 2215 (2018).

266. Monu Bedi, *Social Networks, Government Surveillance, and the Fourth Amendment Mosaic Theory*, 94 B.U. L.J. 1809, 1843–45 (2014) (expressing uncertainty as to the continued use of the public exposure doctrine now that the mosaic theory is applied).

267. *See, e.g.*, United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010) (Sentelle, C.J., dissenting).

268. Katz v. United States, 389 U.S. 347, 352 (1967) (emphasis added).

269. Bedi, *supra* note 266, at 1839–42 (explaining the conceptual difficulties in applying the mosaic theory).

270. Monu Bedi, *The Curious Case of Cell Phone Location Data: Fourth Amendment Doctrine Mash-Up*, 110 NW. U. L. REV. 61, 73 (2015) [hereinafter *Cell Phone Location Data & the Fourth Amendment*] (discussing historical cell-site location information in the context of the third-party doctrine and public exposure doctrine).

271. *Id.* at 73–74.

cell-site location information, irrespective of whether the information concerns past movements, is analogous to "obtaining testimony from an eyewitness," making the collection of public information, available for all to see, lawful.[272] The scholar adds that historical cell-site location information is akin to non-content information necessary to establish communication, and because observing non-content information does not implicate the Fourth Amendment, neither should historical cell-site location information that does not consist of protected content.[273] Lower courts have also held that historical cell-site location information is subject to the public exposure doctrine and therefore does not violate the Fourth Amendment.[274] Limiting the public exposure doctrine to only contemporaneous observations is to say that the information conveyed to the public on any given day is forgotten the moment an individual exits the public sphere. Suppose a friend invites you to a barbeque. At the barbeque, another friend approaches you and mentions seeing you at Costco last week. Using this very simple example, *Katz* teaches us that what becomes public knowledge remains public knowledge. The same is true in the digital arena.[275] If a drunk tweet is posted onto Twitter, deleting the tweet the next morning does not mean the information contained in the tweet will not resurface a day, week, month, or even year later.

The answer to observing historical information, including movements that generate cell-site location information, lies at the heart of *Katz*. The expectations of privacy test was designed to protect that which is deliberately concealed from the government, not that which is clearly exposed to the curious.[276] Public visual surveillance should not, and under *Katz* could not,

---

272. Brief of Professor Orin S. Kerr at 3–7, as Amici Curiae in Support of Respondent, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402).

273. *Fourth Amendment & the Internet*, *supra* note 28, at 1009–11, 1017–22.

274. *See, e.g.*, *In re* United States for an Order Directing Provider of Elec. Commun. Serv. To Disclose Records to the Gov't, 620 F.3d 304, 312–13 (3d Cir. 2010).

275. *See, e.g.*, United States v. Meregildo, 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012) (explaining that the moment the individual shared information on Facebook, that individual's "legitimate expectation of privacy ended."); *see, e.g.*, United States v. Gatson, No. 13–705, 2014 U.S. Dist. LEXIS 173588, at *60 (D.N.J. Dec. 16, 2014) (finding no legitimate expectation of privacy in photos shared to Instagram).

276. *See* Katz v. United States, 389 U.S. 347, 351–52 (1967); *see also id.* at 361 (Harlan, J., concurring).

implicate the Fourth Amendment.[277] The Supreme Court's continued assessment of the length of law enforcement surveillance is a direct departure from the common practice of physical surveillance.[278] For this reason, to hold otherwise is unprecedented and will prove unworkable.

C. Using Technology to Obtain What is Publicly Observable is Consistent With Katz

Using technology to obtain what is already public knowledge is permissible. For example, law enforcement routinely obtains information on drivers in public by recording their license plate information with mobile data terminals that are equipped in most patrol vehicles.[279] Since license plates are publicly displayed, "[t]hey are there for all the world to see, including the world of law enforcement."[280] The Supreme Court has similarly spoken on this issue in *New York v. Class*, where the Court emphasized that "[t]he exterior of a car, of course, is thrust into the public eye, and thus to examine it does not constitute a "'search.'"[281] Although *Class* dealt with a vehicle identification number rather than a license plate number, lower courts insist that *Class* "applies with equal force to license plates."[282]

---

277. *Compare* Kerr, *supra* note 68, at 335 (questioning whether "visual surveillance [should] be subject to" the Fourth Amendment), *with* Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727, 757 (1993) (advocating that visual surveillance should be subject to the Fourth Amendment).

278. *See* David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J. L. & TECH. 381, 403–05 (2013) (noting that visual surveillance is "commonplace" and widely accepted).

279. *See, e.g.*, United States v. Ellison, 462 F.3d 557, 565 n.2 (6th Cir. 2006) (quoting Darlene Cedrés, *Mobile Data Terminals and Random License Plate Checks: The Need for Uniform Guidelines and a Reasonable Suspicion Requirement*, 23 RUTGERS COMPUTER & TECH. L.J. 391, 395–97 (1997) (explaining that "[a] mobile data terminal ('MDT') is a 'remote portable computer' that 'enables the transmission of data between the MDT and a host computer system,' allowing the police access to a multitude of information about a vehicle and its owner by entering in the vehicle's license-plate number.")).

280. State v. Myrick, 282 N.J. Super. 285, 293 (N.J. Super. Ct. App. Div. 1995).

281. New York v. Class, 475 U.S. 106, 114 (1986) (explaining that "it is unreasonable to have an expectation of privacy in an object required by law to be located in a place ordinarily in plain view from the exterior of the automobile.").

282. *See, e.g.*, *Ellison*, 462 F.3d at 561 (holding that "an automobile's Vehicle Identification Number, located inside the passenger compartment, but visible from outside the car, does not receive Fourth Amendment protection."); United States v. Walraven, 892 F.2d 972, 974 (10th Cir.

The technology used in *Carpenter*, namely the data gathered and stored by wireless providers, "merely captured information" that Carpenter had already "exposed to the public."[283] Consequently, as the Court explained in *Knotts*, the use of technology merely enhances law enforcement's ability to obtain information that could have been obtained by public observation,[284] and the use of technology to obtain this information does not violate the expectations of privacy test.[285] The same ruling should have applied in *Carpenter*. According to the majority in *Carpenter*, "the retrospective quality of the data here gives police access to a category of information otherwise unknowable."[286] But law enforcement obtained information on Carpenter's public whereabouts that *was* otherwise knowable through traditional investigatory surveillance methods. For example, if law enforcement physically surveilled Carpenter, law enforcement would have had first-hand knowledge of Carpenter's location in public. If law enforcement obtained video footage of nearby shops, the footage may have revealed Carpenter's location in public. Had there been camera polls affixed in the surrounding area, and law enforcement reviewed them, Carpenter's location in public could have been revealed. Such options are but a few examples of the many ways that law

---

1989) (holding that because license plates "are in plain view, no privacy interest exists in license plates."); Olabisiomotosho v. City of Houston, 185 F.3d 521, 529 (5th Cir. 1999) (holding that "[a] motorist has no privacy interest in her license plate number.").

283. *See, e.g.*, People v. Diaz, 213 Cal. App. 4th 743, 757–58 (Cal. Ct. App. 2013) (finding no reasonable expectation of privacy in the historic speed and braking data taken from the vehicle's sensing diagnostic module because "others could observe [the] vehicle's movements, braking, and speed, either directly or through the use of technology such as radar guns or automated cameras," and the "technology merely captured information . . . knowingly exposed to the public[.]"); Mobley v. State, 346 Ga. App. 641, 646 (Ga. Ct. App. 2018) (finding no reasonable expectation of privacy in the data obtained by the vehicle's airbag control module, like the historical data of a vehicle's speed, "because individuals knowingly expose such information to the public. While an outside observer cannot ascertain the information regarding the use and functioning of a vehicle with the same level of precision as that captured by the ACM, there are outward manifestations of the functioning of some of the vehicle's systems when a vehicle is operated on public roads. For example, a member of the public can observe a vehicle's approximate speed; observe whether a vehicle's brakes are being employed by seeing the vehicle slow down or stop or the brake lights come on, by hearing the sounds of sudden braking; and observe whether the driver is wearing a seatbelt.").

284. United States v. Knotts, 460 U.S. 276, 285 (1983) (explaining that "[a] police car following [the suspect] at a distance throughout his journey could have observed him.").

285. *Id.* at 282, 285.

286. Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

enforcement could have obtained Carpenter's location history, thereby making his location history knowable. Simply put, *Carpenter*'s ruling should have read that "technology merely captured information . . . knowingly exposed to the public[.]"[287] Whether the information concerned the historical data of a vehicle's speed,[288] or the historical cell-site location information, the same conclusion would be reached: individuals lack an expectation of privacy in their public location information. As the dissent indicated in *United States v. Jones*,[289] "[t]he sum of an infinite number of zero-value parts is also zero."[290]

VI. CONCLUSION

"What is left of the Fourth Amendment?"[291] The digital era we live in today allows society to work, shop, socialize, and even monitor one's health without having to leave the confines of one's home. With physical information becoming increasingly digitized, to what extent can the third-party doctrine remain viable? It seems clear that as society becomes increasingly dependent on third parties, the more at-risk society is in having their identity recorded and stored indefinitely. While the use of third parties may be necessary to keep up with "modern society,"[292] determining the reasonable expectations of privacy in shared information is best suited under the public exposure doctrine.

The best solution is to get rid of the "ill suited"[293] third-party doctrine, and instead adhere to *Katz*' public exposure doctrine formula. The lessons of *Carpenter* encourage the active participation with the rest of society beyond the four corners of a home. The Court incentivizes individuals to enter the public sphere with some amount of comfort in knowing that law enforcement may have to alter their surveillance practices in order to observe an

287. *Diaz*, 213 Cal. App. at 757–58.

288. *See Mobley*, 346 Ga. App. at 646.

289. United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010).

290. *Id.*

291. *Carpenter*, 138 S. Ct. at 2262 (Gorsuch, J., dissenting).

292. *Id.* at 2220 (majority opinion).

293. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

individual's journey, for example, to Dodger Stadium. What enters the public, however, is public knowledge. For that reason, what becomes public knowledge remains public knowledge. This common understanding does not change in the eyes of physical information or digital information. The expectation is not that parking in the doctor's parking lot will be kept from any passerby, including law enforcement; it is that the contents of the communication with the doctor will remain private. No amount of days, weeks, or months observing an individual parking at the doctor's parking lot would reveal the intimate contents of the conversation, for it is the contents spoken in a manner deliberately withheld from the public that society regards as reasonably shielded from public knowledge. Because "the sum of an infinite number of zero-value parts is"[294] zero, the mosaic theory should—and under *Katz* must—be rejected. Until then, *Carpenter* will keep law enforcement and "judges guessing for years to come."[295]

294. *Jones*, 625 F.3d at 769.

295. Sykes v. United States, 564 U.S. 1, 34 (2011) (Scalia, J., dissenting); *Carpenter*, 138 S. Ct. at 2234 (Kennedy, J., dissenting) (emphasizing that the majority's decision will result in lower courts "guessing for years to come.").