
THE RUTGERS UNIVERSITY LAW REVIEW
VOLUME 73 | ISSUE 3 SPRING 2021

ONE SMALL STEP, BUT NO GIANT LEAP: HOW *CARPENTER V. UNITED STATES* FAILED TO INCREASE CELL PHONE PRIVACY

Jennifer Nairn[*]

TABLE OF CONTENTS

I. INTRODUCTION

Cell phone activity remains largely unprotected by the Fourth Amendment. This fact undoubtedly makes cell phone users apprehensive at the large swathes of cell phone activity such as emails, internet browsing, and social media use readily available for warrantless government intrusion. The complicated relationship between decades old doctrines and the rapid pace of technological advancements has enabled increasing cell phone privacy to elude the Supreme Court until 2018. The Supreme Court granted certiorari in *United States v. Carpenter* in a case that was the first of its kind: a Fourth Amendment challenge to the warrantless collection of cell site location information ("CSLI"). The

[*] J.D., Rutgers Law School—May 2021. A sincere thank you to Associate Professor Adnan A. Zulfiqar for his guidance and thoughtful commentary on this Note. I am deeply grateful for my supportive community, including my family, friends, and colleagues. Dedicated to my daughter, Avery, and my late grandfather, both of whom have made a profound and everlasting impact on my life.

country waited with bated breath hoping for a leap in cell phone privacy. What it got was a narrow opinion that is only one small piece of a large, complicated puzzle.

Part II of this Note will provide a background regarding Fourth Amendment jurisprudence prior to the *Carpenter* decision. Part III will discuss the *Carpenter* decision and its impact on obtaining CSLI. Next, Part IV contains an analysis of how lower courts are declining to apply the holding in *Carpenter* to other types of cell phone technology. Part V will discuss the shortcomings of the *Carpenter* decision, and Part VI suggests about how the opinion as it stands can be used to create better cell phone privacy.

II. TRACKING THE FOURTH AMENDMENT PRE-*CARPENTER*

The Fourth Amendment of the United States Constitution states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[1]

The Fourth Amendment sets out to protect "the right of the people"[2] but has also been the subject of extensive interpretation since its adoption.[3] Generally, it is recognized that the Fourth Amendment requires the government to have probable cause in order to obtain a warrant that allows a search and seizure to take place.[4] If the government does not have a warrant, the search is per se unconstitutional.[5] One common remedy for an unconstitutional search is known as the exclusionary rule.[6] The exclusionary rule is powerful and

1. U.S. CONST. amend. IV.

2. *Id.*

3. *See* Barry Friedman, *What the Fourth Amendment Fundamentally Requires*, INTERACTIVE CONST., https://constitutioncenter.org/interactive-constitution/interpretation/amendment-iv/interps/121#the-basics-of-the-fourth-amendment (last visited July 5, 2021).

4. Barry Friedman & Orin Kerr, *The Fourth Amendment*, INTERACTIVE CONST., https://constitutioncenter.org/interactive-constitution/interpretation/amendment-iv/interps/121 (last visited July 5, 2021).

5. Katz v. United States, 389 U.S. 347, 357 (1967). Exceptions to the warrant requirement, such as search incident to arrest, exigency, etc., will not be discussed in this Note.

6. *See* Weeks v. United States, 232 U.S. 383, 398 (1914).

prevents the use of illegally seized evidence in a criminal trial.[7] The rule's origin dates back to 1914 when the Supreme Court held that a warrantless search of a defendant's home violated his constitutional rights, and therefore the evidence seized during this search must be returned to the defendant.[8] In *Weeks v. United States*, the defendant was charged with nine violations, including the use of mail to transport coupons representing chances at the lottery.[9] He was arrested without a warrant, and police searched his home twice without a warrant.[10] During the searches, police seized various papers and letters belonging to the defendant.[11] The defendant's petition for the return of his possessions was denied, and they were used in his trial.[12] The Court declared that the searches violated the defendant's constitutional rights and thus the lower court should have returned the defendant's possessions.[13] In its opinion, the Court reasoned:

> If letters and private documents can thus be seized and held and used in evidence against a citizen accused of an offense, the protection of the 4th Amendment, declaring his right to be secure against such searches and seizures, is of no value, and, so far as those thus placed are concerned, might as well be stricken from the Constitution. The efforts of the courts and their officials to bring the guilty to punishment, praiseworthy as they are, are not to be aided by the sacrifice of those great principles established b[y] years of endeavor and suffering which have resulted in their embodiment in the fundamental law of the land.[14]

Although it does not expressly discuss the exclusionary rule, *Weeks* is still viewed as the origin of this rule.[15] In 1961, the Supreme Court held that the exclusionary rule not only applied in federal courts, but also extended to state courts as well.[16]

7. *Exclusionary Rule's Critical Role*, WASH. TIMES (OCT. 5, 2008), https://www.washingtontimes.com/news/2008/oct/05/exclusionary-rules-crucial-role/.

8. *Weeks*, 232 U.S. at 398.

9. *Id.* at 386.

10. *Id.* at 386–87. The arrest and searches occurred before the defendant was indicted. *Id.* at 398.

11. *Id.* at 386–87.

12. *Id.* at 389.

13. *Id.* at 398.

14. *Id.* at 393.

15. Donald L. Doernberg, *"The Right of the People": Reconciling Collective and Individual Interests Under the Fourth Amendment*, 58 N.Y.U. L. REV. 259, 272–73 (1983).

16. Mapp v. Ohio, 367 U.S. 643, 659–60 (1961) ("The ignoble shortcut to conviction left open to the State tends to destroy the entire system of constitutional restraints on which the liberties of the people rest."). The exclusionary rule was later expanded into the "Fruit

With the foundation laid for understanding a probable cause warrant is required for a search and seizure and the remedy for any violations, another important component of understanding Fourth Amendment jurisprudence on the path to *Carpenter* is how the courts have interpreted "unreasonable searches and seizures."[17] In 1928, the Supreme Court held that the Fourth Amendment referred only to searches of physical things in *Olmstead v. United States*.[18] The defendant in *Olmstead* was under suspicion for being the leader of a conspiracy to import and distribute alcohol.[19] Federal prohibition officers acquired the majority of the information in their investigation by wiretapping the defendant's telephone and listening to private conversations for several months.[20] The Court concluded that, consistent with precedent at the time, the plain text of the Fourth Amendment referred only to material things[21] and further specified that it could not justify extending the meaning of searches and seizures to prevent hearing and sight being used to obtain information.[22] As such, the wiretapping was neither a search nor a seizure.[23]

Justice Brandeis authored a famous dissent in *Olmstead* that criticized the narrow interpretation of the Fourth Amendment, citing the Framers' intent in protecting Americans against the government when drafting the Constitution.[24] He wrote:

> The protection guaranteed by the amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and

of the Poisonous Tree" Doctrine, which was first introduced by the Supreme Court in *Silverthorne Lumber Co. v. United States*, 251 U.S. 385 (1920). Gary D. Spivey, Annotation, *"Fruit of the Poisonous Tree" Doctrine Excluding Evidence Derived from Information Gained in an Illegal Search*, 43 A.L.R.3d § 3 (1972). This Doctrine excludes "evidence derived from information gained in an illegal search." *Id.*

17. U.S. CONST. amend. IV.

18. 277 U.S. 438, 464 (1928).

19. *Id.* at 455.

20. *Id.* at 456–57. It is important to note that the wiretapping was set up without any trespass onto the defendant's property. *Id.* at 457.

21. "Neither the cases we have cited nor any of the many federal decisions brought to our attention hold the Fourth Amendment to have been violated as against a defendant, unless there has been an official search and seizure of his person or such a seizure of his papers or his tangible material effects or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure." *Id.* at 466.

22. *Id.* at 465.

23. *See id.* at 466.

24. *See id.* at 478 (Brandeis, J., dissenting).

> satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect, that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.[25]

Justice Brandeis focused his dissent on a broad interest in maintaining liberty and privacy that is free from government intrusion, whether it involves a physical intrusion or not.[26]

It was not until 1967 that the Supreme Court finally overruled *Olmstead* and expanded the interpretation of search and seizure beyond a physical intrusion.[27] In *Katz v. United States*, the Supreme Court embraced the broad scope of protection suggested in Justice Brandeis's dissenting opinion nearly forty years earlier, thus eliminating the requirement for a search and seizure to take place in one's home in order for it to be deemed unreasonable.[28] The Court redefined the scope of the Fourth Amendment as protecting "people, not places" and specified that "the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion."[29] The Court went on to quantify this new scope, indicating 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. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[30] A concurring opinion authored by Justice Harlan in *Katz* suggested a two-prong requirement for determining when a person should be afforded this constitutional protection.[31] The requirements are a subjective expectation of privacy and that the expectation is objectively reasonable.[32]

The Court's use of the reasonable expectation of privacy test has its limitations.[33] The third-party doctrine provides that there is no reasonable expectation of privacy in disclosures to third parties.[34]

25. *Id.*
26. *Id.* at 479.
27. *See* Katz v. United States, 389 U.S. 347, 353 (1967).
28. *Id.* at 359.
29. *Id.* at 351, 353.
30. *Id.* at 351 (citations omitted).
31. *Id.* at 361 (Harlan, J., concurring).
32. *Id.*
33. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).
34. *Id.*

This doctrine stemmed from two types of cases: confidential informants in 1952–71 and business records in 1973–80.[35] In multiple cases involving confidential informants, the Supreme Court focused on the voluntary nature of the disclosures of wrongdoing made by the defendants, as well as the negative impact on investigation of organized crime and the inequity in extending constitutional protection in these situations.[36] The business records cases before the Supreme Court involved a variety of different types of records given to a third party: tax documents given to an accountant,[37] financial documents given to a bank,[38] and telephone records.[39] The Supreme Court consistently held that information voluntarily transmitted to a third party was no longer afforded Fourth Amendment protection because there was no longer an expectation of privacy.[40]

While the third-party doctrine is controversial and widely criticized,[41] a compelling argument in support of this doctrine is that it allows for consistency with Fourth Amendment decisions.[42] One simply does not have a reasonable expectation of privacy in anything that is voluntarily disseminated.[43]

An early criticism of the third-party doctrine concerned the concept of voluntariness.[44] Justice Brennan voiced his concerns in a 1976 Supreme Court case involving bank records falling under the third-party doctrine: "For all practical purposes, the 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."[45]

The digital age has further called into question not only the aspect of the degree of voluntary disclosure, but also the validity of the entire third-party doctrine.[46] In a 2012 Supreme Court case involving global

35. *Id.* at 566–69.

36. *Id.*

37. Couch v. United States, 409 U.S. 322, 335–36 (1973).

38. United States v. Miller, 425 U.S. 435, 437–38 (1976).

39. Smith v. Maryland, 442 U.S. 735, 741–42 (1979).

40. Kerr, *supra* note 33, at 567–68.

41. *Id.* at 573 (referencing "widespread criticism of the third-party doctrine"); RICHARD M. THOMPSON II, CONG. RSCH. SERV., R43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE 2 (2014) (describing the third-party doctrine as "heavily criticized").

42. RICHARD M. THOMPSON II, CONG. RSCH. SERV., R43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE 15 (2014).

43. *Id.*

44. United States v. Miller, 425 U.S. 435, 447–52 (1976) (Brennan, J., dissenting).

45. *Id.* at 451 (quoting Burrows v. Superior Court, 13 Cal. 3d 238, 247 (1974)).

46. Orin Kerr & Greg Nojeim, *The Data Question: Should the Third-Party Records Doctrine Be Revisited?*, A.B.A. J. (Aug. 1, 2012, 9:20 AM), http://www.abajournal.com/

positioning system ("GPS") technology, Justice Sotomayor expressed concerns about the doctrine:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.[47]

Critics of the doctrine in this digital age have suggested that its application in this era leads to "absurd results" because of the way technology funnels information through intermediaries.[48]

> The doctrine was forged at a time very different from our own. There was no email, and people communicated primarily by phone, fax and letter. There was no World Wide Web—if you wanted to find merchandise, you used the Yellow Pages. Cellular telephones were the stuff of science fiction. To put the period in perspective, the Vietnam War was winding down, Americans heard their music on eight-track tapes, and the Chevy Nova and Ford Maverick were the leading car models.[49]

The crux of the criticism levied against the third-party doctrine hinges on what is considered a voluntary disclosure when it comes to digital information.[50] A cell phone user may voluntarily download and interact with a smartphone application, thus suggesting an understanding that this use is transmitted to a third party.[51] However, that interaction with the application is controlled at the sole, voluntary discretion of the phone user. The analysis is more complicated when it is necessary to determine how voluntary the disclosure of something like metadata or technology such as cell site location information ("CSLI") really is.[52] If a user does not know that a cell phone can transmit this

magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited.

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

48. Kerr & Nojeim, *supra* note 46.

49. *Id.*

50. *See* Margaret E. Twomey, Note, *Voluntary Disclosure of Information as a Proposed Standard for the Fourth Amendment's Third-Party Doctrine*, 21 MICH. TELECOMM. & TECH. L. REV. 401, 416–18 (2015).

51. *Id.* at 417–18.

52. *Id.* at 417.

data to a third party, the foundational voluntary component of the third-party doctrine is called into question.[53] A strict application of the third-party doctrine would lead to the conclusion that accessing metadata is *not* a search and, therefore, not afforded any Fourth Amendment protection. The tension created by the application of a doctrine established in the 1970s to rapidly developing twentieth-century technology was a scenario ripe for resolution. The stage was set for a case like *Carpenter*.

III. *CARPENTER V. UNITED STATES*

In June 2018, the Supreme Court held for the first time that the government's access of CSLI constituted a search under the Fourth Amendment.[54] Four men were arrested in 2011 for robbing multiple Radio Shack and T-Mobile stores.[55] One of the men admitted to being part of a large group who robbed nine stores in Michigan and Ohio over the course of the four months prior and identified fifteen individuals who also participated.[56] He subsequently provided police some phone numbers of the accomplices, and authorities reviewed his phone records.[57] Prosecutors applied for court orders pursuant to the Stored Communications Act[58] to obtain Timothy Carpenter's cell phone records.[59] Federal Magistrate Judges granted two orders to obtain CSLI from his cell phone carriers over the course of the four-month period.[60] CSLI is data collected by wireless carriers when cell phones search for cell sites, usually on towers, for a signal.[61] Each cell site antenna delivers cell service for either 60 degrees or 120 degrees of a circular geographic area.[62] Once a cell phone connects to a cell site, it creates a time stamped

53. Orin Kerr, *Eleventh Circuit, Disagreeing with the Fifth, Holds Fourth Amendment Protects Cell-Site Records*, WASH. POST: VOLOKH CONSPIRACY (June 11, 2014, 7:32 PM), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/11/eleventh-circuit-disagreeing-with-the-fifth-holds-fourth-amendment-protects-cell-site-records.

54. Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).

55. *Id.* at 2212.

56. *Id.*

57. *Id.*

58. "That statute, as amended in 1994, permits the Government to compel the disclosure of certain telecommunications records when it 'offers specific and articulable facts showing that there are reasonable grounds to believe' that the records sought 'are relevant and material to an ongoing criminal investigation.'" *Id.* (quoting 18 U.S.C. § 2703(d)). "Reasonable grounds" is a standard well below the probable cause required for a search warrant. *Id.* at 2221.

59. *Id.* at 2212.

60. *Id.*

61. *Id.* at 2211–12.

62. *Id.* at 2225 (Kennedy, J., dissenting).

record known as CSLI.[63] This record exposes the general area of the cell phone.[64] The government obtained a staggering 12,898 location points, averaging "101 data points per day" from the orders.[65] These data points created a record tracing Carpenter's movements during this period of time.[66] Carpenter received twelve criminal charges: six charges of robbery and six charges of "carrying a firearm during a federal crime of violence."[67]

Carpenter moved to suppress the CSLI data prior to trial on the basis that it constituted a warrantless search, but the motion was denied.[68] Carpenter was convicted and sentenced to more than 100 years in prison.[69] The CSLI data played a key role in Carpenter's conviction, providing a map of Carpenter's phone near each of the four robberies.[70] On appeal, the Court of Appeals for the Sixth Circuit affirmed that Carpenter lacked a reasonable expectation of privacy in the CSLI.[71] Because "cell phone users voluntarily convey cell-site data to their carriers as 'a means of establishing communication,' the court concluded that the resulting business records are not entitled to Fourth Amendment protection."[72] The Court of Appeals essentially applied the same logic from a 1979 Supreme Court case involving landline telephone records[73] to 2011 mobile phone technology unavailable when the earlier case was decided.[74] This application allows searches of CSLI without establishing probable cause for a warrant. The Supreme Court granted certiorari in 2017.[75]

The Supreme Court began its opinion with a brief summary of Fourth Amendment protection that provided the framework for its decision.[76] When "an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,'" a search occurs under the Fourth Amendment which

63. *Id.* at 2211 (majority opinion).
64. *Id.* at 2225 (Kennedy, J., dissenting).
65. *Id.* at 2212 (majority opinion).
66. *Id.*
67. *Id.*
68. *Id.*
69. *Id.* at 2213.
70. *Id.* at 2212–13.
71. *Id.* at 2213.
72. *Id.* (quoting United States v. Carpenter, 819 F.3d 880, 888 (2016)).
73. Smith v. Maryland, 442 U.S. 735, 741 (1979).
74. *See The First Mobile Phone Call Was Placed 40 Years Ago Today*, FOX NEWS (Apr. 3, 2013), https://www.foxnews.com/tech/the-first-mobile-phone-call-was-placed-40-years-ago-today (discussing how the first mobile phone call was made in 1973, but mobile phones were not available to consumers until 1983).
75. *Carpenter*, 138 S. Ct. at 2213.
76. *Id.* at 2213–14.

requires a warrant to avoid a government intrusion.[77] Given that there is no single definition of expectations of privacy, the Court enumerated two foundational principles: (1) that the Fourth Amendment protects the "privacies of life" from "arbitrary power"[78] and (2) the objective of the Framers "to place obstacles in the way of a too permeating police surveillance."[79]

The Court opined that CSLI does not fit squarely within the two types of cases dealing with Fourth Amendment privacy: physical location and movement and information voluntarily disclosed to third parties.[80] While the Court conceded that this scenario could trigger the third-party doctrine, it questioned the doctrine's applicability to CSLI:

> 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. After all, when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements.[81]

The Court has long defended that one has "a reasonable expectation of privacy in the whole of their physical movements,"[82] even when those movements take place in public.[83] Since cell phones have become such a ubiquitous part of daily life and accompany users nearly everywhere, CSLI provides "near perfect surveillance" of one's location[84] that is "detailed, encyclopedic, and effortlessly compiled."[85] It also "provides an intimate window into a person's life, revealing not only his physical movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[86] Furthermore, the Court also questioned the voluntary aspect of the third-party doctrine in its applicability to CSLI.[87] Specifically, the Court focused on the idea that

77. *Id.* at 2213 (quoting *Smith*, 442 U.S. at 740).
78. *Id.* at 2214 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).
79. *Id.* (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).
80. *Id.* at 2214–16.
81. *Id.* at 2216–17.
82. *Id.* at 2217 (citing United States v. Jones, 565 U.S. 400, 430 (2012); Katz v. United States, 389 U.S. 347, 351–52 (1967)).
83. *Id.*
84. *Id.* at 2218.
85. *Id.* at 2216.
86. *Id.* at 2217 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).
87. *Id.* at 2220.

cell phones are essential in modern society and require no affirmative act by the user in order to create CSLI.[88]

Historically, surveillance performed by law enforcement was limited to brief periods of time due to difficulty and expense and, therefore, created an expectation that law enforcement could not track an individual for a long period of time.[89] Permitting the government access to CSLI would violate that expectation.[90]

> Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection. Whether the Government employs its own surveillance technology . . . or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. The location information obtained from Carpenter's wireless carriers was the product of a search.[91]

The Court held that the third-party doctrine did not apply to CSLI since it is an "entirely different species of business record."[92]

The Court referenced Justice Brandeis's dissent from *Olmstead* in justifying its decision. "[T]he Court is obligated—as '[s]ubtler and more far-reaching means of invading privacy have become available to the Government'—to ensure that the 'progress of science' does not erode Fourth Amendment protections."[93] Despite acknowledging its obligations as set forth by Justice Brandeis and regarding the problematic nature of applying the established doctrine to cell phone technology, the Court warned:

> Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or "tower dumps" (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of *Smith* and *Miller* or call into question

88. *Id.*

89. *Id.* at 2217 (citing *Jones*, 565 U.S. at 429–30 (Alito, J., concurring)).

90. *Id.*

91. *Id.* The Court specified that accessing seven or more days of CSLI constitutes a search. *Id.* at 2217 n.3. Since this is considered a search, a warrant is now required before obtaining CSLI records for greater than six days. *Id.*

92. *Id.* at 2217, 2222.

93. *Id.* at 2223 (quoting Olmstead v. United States, 277 U.S. 438, 473–74 (1928) (Brandeis, J., dissenting)).

> conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security.[94]

The Court concluded by specifying that due to "the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection."[95]

It is unsurprising that this decision generated four dissenting opinions. Justice Kennedy called for a strict application of the third-party doctrine, opining that cell site records are no different from other business records because they are "created, kept, classified, owned, and controlled by cell phone service providers"[96] and, therefore, an individual does not have any reasonable expectation of privacy in those records.[97] Justice Kennedy was also critical of the majority's implication that privacy interests should be weighed against the type of information disclosed.[98] He further opined that the general location indicated by the CSLI is no more revealing than traditional business records, such as bank records.[99]

Justice Thomas dissented on the grounds that the majority should not have been determining whether a search occurred, but rather whose property was searched.[100] He concluded that the majority erred when it determined that although the cell site records belonged to the cell phone company, Carpenter still maintained a reasonable expectation of privacy in them.[101] The effect of this is that "individuals can claim a reasonable expectation of privacy in someone else's business records."[102]

Justice Alito was also critical of the majority's determination that an individual has a reasonable expectation of privacy in third-party business documents.[103] In his dissent, he opined that the majority's classification of the government obtaining cell site records pursuant to

94. *Id.* at 2220.
95. *Id.* at 2223.
96. *Id.* at 2229 (Kennedy, J., dissenting).
97. *Id.* at 2231–32.
98. *Id.* at 2232.
99. *Id.* at 2232–33.
100. *Id.* at 2235 (Thomas, J., dissenting).
101. *Id.* at 2235–36.
102. *Id.* at 2242.
103. *Id.* at 2257 (Alito, J., dissenting).

an order as a search ignores an understanding of the Fourth Amendment.[104] Justice Gorsuch agreed with the majority that the rationale of the third-party doctrine is incorrect.[105] "Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers."[106] The third-party doctrine is ill-suited for this era, and strict construction of it leads to the conclusion that the government can access all of the formerly private data that is "now resid[ing] on third party servers."[107] However, Justice Gorsuch's criticism that the majority merely put the third-party doctrine on "life support"[108] hardly provided any dispositive guidance for the future.

IV. APPLYING *CARPENTER* IN THE LOWER COURTS

The majority opinion in *Carpenter* provided framework for its determination that CSLI deserves Fourth Amendment protection. One has a reasonable expectation of privacy in "the record of his physical movements"[109] to avoid exposure of "familial, political, professional, religious, and sexual associations."[110] The Court described CSLI's "deeply revealing nature . . . its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection" in justifying the conclusion that it warrants Fourth Amendment protection.[111]

While *Carpenter* was initially lauded as a success in the endeavor for cell phone privacy rights,[112] it is critical to examine how lower courts have used the framework in deciding subsequent cases involving cell phone technology to determine whether *Carpenter* has created a significant increase in cell phone privacy.[113] The importance of measuring the impact

104. *Id.* at 2247.
105. *Id.* at 2272 (Gorsuch, J., dissenting).
106. *Id.* at 2262.
107. *Id.*
108. *Id.* at 2272.
109. *Id.* at 2217 (majority opinion).
110. *Id.* (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (internal quotations omitted)).
111. *Id.* at 2223.
112. Curt Levey, *Supreme Court Ruling in Cell Phone Case is a Victory for Our Privacy Rights*, FOX NEWS (June 22, 2018), https://www.foxnews.com/opinion/supreme-court-ruling-in-cell-phone-case-is-a-victory-for-our-privacy-rights.
113. *See* Anthony G. Amsterdam, *The Supreme Court and the Rights of Suspects in Criminal Cases*, 45 N.Y.U. L. REV. 785, 786 (1970) ("The significance of the Court's pronouncements—their power to shake the assembled faithful with awful tremors of exultation and loathing—does not depend upon their correspondence with reality. Once uttered, these pronouncements will be interpreted by arrays of lower appellate courts, trial

on digital privacy cannot be overstated. The number of requests received by cell phone carriers for location information is tremendous. In the first half of 2019, Verizon received 136,034 total demands for information.[114] Similarly, AT&T received 133,695 total demands for information during that same timeframe.[115]

The Court expressed that the *Carpenter* decision was narrow and only articulated an opinion related to CSLI.[116] This, however, does not preclude the possibility that the *Carpenter* framework can be applied to other types of cell phone technology to protect them from warrantless searches. Given the vast functions a cell phone can serve beyond telephone calls and text messaging,[117] it is possible that the *Carpenter* framework can apply to a wide variety of technology.

First, *Carpenter* emphasized that it was leaving real-time CSLI and cell tower dumps open to interpretation,[118] but this created a disparity in how courts are handling these situations.

In 2019, the United States District Court for the District of Kansas pointed out the lack of clarity the *Carpenter* decision created regarding real-time CSLI when denying that the framework applies:

> But, *Carpenter* specifically left open the question whether seizing CSLI in real-time was entitled to Fourth Amendment protection. And, extending *Carpenter*'s holding about the seizure of historical CSLI to the seizure of real-time CSLI is far from clear because *Carpenter* emphasized that historical CSLI allowed the government to learn of a person's whereabouts on a nearly 24-hour, seven-day-a-week basis. Meanwhile, seizing CSLI in real-time only reveals a person's whereabouts at the moment of its seizure.[119]

judges, magistrates, commissioners and police officials. *Their* interpretation . . . for all practical purposes, will become the word of god.").

114. *United States Report*, VERIZON, https://www.verizon.com/about/portal/transparency-report/us-report/ (last visited Jan. 4, 2020).

115. AT&T, AT&T AUGUST 2019 TRANSPARENCY REPORT 3 (2019), https://about.att.com/ecms/dam/csr/2019/library/transparency/2019-August-Report.pdf.

116. 138 S. Ct. at 2220–21.

117. For a discussion on unique services provided by cell phones, including car trouble diagnostics, playing a favorite television show, measuring blood alcohol content, and much more, see Sarah Crow, *20 Things You Didn't Know Your Smartphone Could Do*, BESTLIFE (May 15, 2018), https://bestlifeonline.com/surprising-smartphone-features/.

118. 138 S. Ct. at 2220.

119. United States v. Thompson, No. 13-40060-10-DDC, 2019 WL 3412304, at *7 (D. Kan. July 29, 2019) (citation omitted).

The Texas Court of Criminal Appeals even specifically stated that cases involving real-time CSLI needed to be decided on an individual basis because *Carpenter* failed to provide defined parameters for dealing with real-time CSLI.[120] In that case, the court applied the framework for historical CSLI to real-time CSLI because *Carpenter* did not provide further guidance:

> Here, Appellant did not have a legitimate expectation of privacy in his physical movements or his location as reflected in the less than three hours of real-time CSLI records accessed by police by pinging his phone less than five times. Five justices on the United States Supreme Court have supported the idea that longer-term surveillance might infringe on a person's legitimate expectation of privacy if the location records reveal the "privacies of [his] life," but this is not that case.[121]

The North Carolina Court of Appeals went as far as to say that *Carpenter only* applies to historical CSLI and does not apply to either real-time CSLI or prospective CSLI.[122]

Similarly, *Carpenter* was expressly non-dispositive regarding cell tower dumps. In *United States v. Adkinson*, the Seventh Circuit Court of Appeals applied the framework used for historical CSLI to tower dumps and concluded that Fourth Amendment protection did not apply.[123] *Carpenter* "did not invalidate warrantless tower dumps (which identified phones near *one location* (the victim stores) at *one time* (during the robberies))."[124] *Carpenter*'s requirement that the technology at issue create a "record of his physical movements"[125] has created a situation where courts are declining to extend Fourth Amendment protection to any technology that does not create a comprehensive record of one's movements.

Social media is one of the most common uses for cell phones.[126] However, the *Carpenter* framework offers no Fourth Amendment protection to social media activity. In 2018, shortly after the *Carpenter*

120. Sims v. State, 569 S.W.3d 634, 645–46 (Tex. Crim. App. 2019).

121. *Id.* at 646 (citation omitted).

122. State v. Thomas, 834 S.E.2d 654, 659 (N.C. Ct. App. 2019) (stating that "[b]ecause *Carpenter* was decided only with respect to historical CSLI, it is dispositive on that issue only").

123. 916 F.3d 605, 610–11 (7th Cir. 2019) (per curiam).

124. *Id.* at 611.

125. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

126. Gordon Donnelly, *75 Super-Useful Facebook Statistics for 2018*, WORDSTREAM (Mar. 5, 2020), https://www.wordstream.com/blog/ws/2017/11/07/facebook-statistics ("19% of time spent on mobile devices occurs on Facebook.").

decision, the United States District Court for the District of New Mexico denied that the *Carpenter* framework applied to social media subscriber information.[127] The United States District Courts for the District of Connecticut[128] and the Northern District of Ohio[129] also issued similar opinions. In each case, the court opined that subscriber information does not fit in the *Carpenter* framework because it does not track one's location over time.[130]

Similar to Facebook subscriber information, *Carpenter* also does not change the treatment of email subscriber information—however, for a different reason.[131] In *United States v. Johnson*, a defendant whose emails were discovered through the subpoena of another's email subscriber information in a child pornography investigation sought to have the evidence suppressed on the basis that *Carpenter* shifted the reasonable expectation of privacy as it relates to electronic messages.[132] The court opined, "the third-party doctrine continues to apply with force . . . . because of [defendant's] intent to 'knowingly expose[] to the public' the contents of his messages by sending them purposefully to another user."[133] Despite *Carpenter*'s discussion of the inadequacies of the third-party doctrine in the digital era,[134] the opinion specifically does not "disturb" the third-party doctrine.[135] The result of this is that it does not actually provide any further protection or privacy for email subscriber information.

127. United States v. Streett, 363 F. Supp. 3d 1212, 1252, 1308 (D.N.M. 2018) (denying *Carpenter* applies to Twitter accounts).

128. United States v. Westley, No. 3:17-CR-171, 2018 WL 3448161, at *14 n.9 (D. Conn. July 17, 2018) (denying *Carpenter* applies to Facebook subscriber information).

129. United States v. Maclin, 393 F. Supp. 3d 701, 706–08 (N.D. Ohio 2019) (denying *Carpenter* applies to Facebook, KIK, and Dropbox subscriber information).

130. *Streett*, 363 F. Supp. 3d at 1308 ("Streett's subscriber information—provides no such insight into Streett's movements."); *Westley*, 2018 WL 3448161, at *14 n.9 (citation omitted) ("The Supreme Court explained that its reasoning was based, in part, on the 'unique nature of cell phone location information' in that it provided 'encyclopedic' information about a person's past movements. No court appears to have held, and I do not find here, that Facebook account subscriber information implicates the concerns raised in *Carpenter*."); *Maclin*, 393 F. Supp. 3d at 708 ("CSLI provides the precise location of Defendant; subscriber information does not.").

131. United States v. Johnson, No. 17-10129-LTS, 2019 WL 917175, at *7 (D. Mass. Feb. 25, 2019).

132. *Id.* at *1, *6.

133. *Id.* at *7 (quoting United States v. Dunning, 312 F.3d 528, 531 (1st Cir. 2002)). Although the court in *Johnson* does not articulate this in its opinion, email subscriber information also does not provide a record of one's personal movements and, therefore, the *Carpenter* framework would not change the treatment of email subscriber information.

134. Carpenter v. United States, 138 S. Ct. 2206, 2216–17 (2018).

135. *Id.* at 2220.

In light of the post-*Carpenter* treatment of email subscriber information, it is unsurprising that the third-party doctrine also still applies to eBay transactions.[136] In *United States v. Schaefer*, the defendant purchased a number of materials on eBay that can be used to make explosives.[137] He requested that the court determine whether the third-party doctrine applies to eBay transactions following the *Carpenter* decision.[138] The court relied on the narrowness of *Carpenter* in determining that the third-party doctrine still applies to eBay transactions since the defendant voluntarily used eBay, which "'exposed' that information."[139] The *Carpenter* decision did not change the fact that the third-party doctrine remains in effect when dealing with eBay transactions, technology which did not exist at the time the doctrine was created.

Courts have also declined to apply the *Carpenter* framework to challenges regarding Internet Protocol Addresses ("IP addresses"), although the reasoning for these determinations has run the gamut. An IP address is a unique identifier assigned to a device that connects to a network.[140] In 2019, the United States District Court for the Northern District of Georgia held that a defendant did not have a reasonable expectation of privacy in his IP address because IP addresses do not provide a precise enough location that would rise to a reasonable expectation of privacy.[141] "IP address information merely shows the location at which a device accesses the internet during a specific session."[142] The court opined that the defendant failed to establish that the IP addresses created an accurate enough record of his location that would track him "into private residences, doctor's offices, political headquarters, and other potentially revealing locales."[143] Incredibly, even though the government in that matter obtained over six months of IP addresses, the court held that it simply did not provide the same "historical portrait of 'the whole of a person's physical movement.'"[144]

136. United States v. Schaefer, No. 3:17-cr-00400-HZ, 2019 WL 267711, at *4–5 (N.D. Or. Jan. 17, 2019).

137. *Id.* at *1.

138. *Id.* at *4.

139. *Id.* at *5 (quoting Smith v. Maryland, 442 U.S. 735, 744 (1979)).

140. *What Is an IP Address?*, IP LOCATION (Feb. 16, 2007), https://www.iplocation.net/ip-address.

141. United States v. Jenkins, No. 1:18-cr-00181, 2019 WL 1568154, at *4–5 (N.D. Ga. Apr. 11, 2019).

142. *Id.* at *4.

143. *Id.* (quoting Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018)).

144. *Id.* at *4–5 (quoting United States v. Monroe, 350 F. Supp. 3d 43, 49 (D.R.I. 2018) (citing *Carpenter*, 138 S. Ct. at 2219)).

The United States District Court for the District of Rhode Island even went as far as to equate IP addresses with records of dialed telephone numbers and, therefore, declared that the third-party doctrine applies since *Carpenter* did not disturb it.[145] The court explained that since an IP address does not provide an "exhaustive chronicle"[146] and "[a]lthough an IP address is a unique numerical identifier, it can only provide 'the location at which one of any number of computer devices may be deployed, much like a telephone number can be used for any number of telephones.'"[147]

The Arizona District Court also held that the third-party doctrine applies.[148] It likened an IP address to a return address on an envelope or a telephone number, neither of which have a privacy interest.[149]

The Fifth Circuit Court of Appeals took a similar approach when it described IP addresses as "business records that might incidentally reveal location information."[150] Therefore, the Fifth Circuit held that the third-party doctrine clearly applied to the IP addresses in that case, meaning the defendant had no reasonable expectation of privacy regarding the IP addresses.[151]

Even beyond the context of cell phones, the *Carpenter* framework also does not apply to pole cameras[152] for similar reasons as tower dumps. In *United States v. Kubasiak*, the defendant argued that a surveillance camera installed by police to record his backyard violated the Fourth Amendment.[153] The court focused on the fact that the camera was in a fixed location, so it did not create the type of record of one's movements that *Carpenter* sought to protect:

> Because the surveillance camera was fixed, it could observe the defendant in only one location—his back yard. It could not track him around the neighborhood. It could not follow him into his doctor's office, or a political headquarters, or a place of worship. It could not follow him inside his home (a place where he had a

145. *Monroe*, 350 F. Supp. 3d at 49.

146. *Id.* at 48 (quoting *Carpenter*, 138 S. Ct. at 2219).

147. *Id.* (citation omitted) (citing In re BitTorrent Adult Film Copyright Infringement Cases, 296 F.R.D. 80, 84 (E.D.N.Y. 2012)).

148. United States v. McCutchin, No. CR-17-01517-001-TUC-JAS, 2019 WL 1075544, at *2 (D. Ariz. Mar. 7, 2019).

149. *Id.* at *3.

150. United States v. Contreras, 905 F.3d 853, 857 (5th Cir. 2018) (quoting *Carpenter*, 138 S. Ct. at 2220).

151. *Id.*

152. United States v. Kubasiak, No. 18-cr-120-pp, 2018 WL 4846761, at *7 (E.D. Wis. Oct. 5, 2018).

153. *Id.* at *1.

> reasonable expectation of privacy). Even for twenty-four hours a day over several months, it could "observe" the defendant only when he was in his backyard, within view of the camera. It might, in that process, capture certain information about the defendant. If he was in the back yard with other people, it would observe those people, and thus provide information about with whom the defendant associated. If he was doing something in his back yard that he would have preferred other people not to see, it would have captured that activity.[154]

The *Carpenter* framework does not apply to toll records and cell phone subscriber information because *Carpenter* only applies when the technology tracks an individual's location for a period of time, instead of a fixed location such as a toll booth.[155]

V. THE FAILURES OF *CARPENTER*

Given the criticism of the third-party doctrine by scholars[156] and Justices[157] alike, *Carpenter* was welcomed with open arms:

> This is the opinion most privacy law scholars and privacy advocates have been awaiting for decades. Oceans of ink have been spilled by those worried about how the dramatic expansion of technologically fueled corporate surveillance of our private lives automatically expands police surveillance too, thanks to the way the Supreme Court has construed the reasonable expectation of privacy test and the third-party doctrine.[158]

Despite the warning that the opinion is "narrow," *Carpenter* was initially described as "a strong first step"[159] and a "potential game changer."[160] The case analysis above suggests that the "oceans of ink"[161] will continue to spill because *Carpenter* has not provided additional privacy against intrusion and surveillance. A wide breadth of technology

154. *Id.* at *6.
155. United States v. Beverly, 943 F.3d. 225, 235 (5th Cir. 2019).
156. Kerr, *supra* note 33 at 563, 573 (referencing "widespread criticism of the third-party doctrine").
157. *See, e.g.*, United States v. Jones, 565 U.S. 400, 417 (Sotomayor, J., concurring).
158. Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 362 (2019).
159. Evan Caminker, *Location Tracking and Digital Data: Can* Carpenter *Build a Stable Privacy Doctrine?*, 2018 SUP. CT. REV. 411, 415 (2019).
160. *Id.* at 413.
161. Ohm, *supra* note 158, at 362.

has come before the courts, and *Carpenter* has not applied to anything other than historical CSLI. There are three main shortfalls of the decision that are demonstrated through the case analysis.

First, the third-party doctrine remains wholly unchanged. Incredibly, the majority expressed significant concerns over the antiquated doctrine but did nothing to change it.[162] The case analysis exemplifies that the doctrine still applies to a wide variety of technology. This includes email subscriber information,[163] eBay transactions,[164] and IP addresses.[165] In particular, IP addresses were analogized to records of dialed telephone numbers[166] and return addresses on envelopes,[167] which shows how the third-party doctrine has not been weakened whatsoever by *Carpenter*.

Second, the threshold for tracking an individual's location is entirely too high. The *Carpenter* decision described CSLI as creating "near perfect surveillance"[168] and in doing so, whether intentionally or not, created a standard for whether one has a reasonable expectation of privacy in location tracking technology that is difficult to meet. This is particularly astonishing when examining the courts' reasonings regarding IP addresses. In one case, the government obtained six months of IP addresses for a defendant but determined that those IP addresses did not track him in the same manner as CSLI because it did not create a record of the "whole" of his movements.[169] This "near perfect surveillance"[170] threshold is so high that even six months of recording every location where an individual connects to a network[171] still is not enough to trigger Fourth Amendment protection according to the *Carpenter* opinion. During the course of six months, a person could connect to a significant number of networks including, but not limited to, one's home, office, or school; the homes of friends or family; and any public place offering a connection such as department stores, restaurants or coffee shops, hotels, museums, airports, and even courthouses. Tracking these network

162. Carpenter v. United States, 138 S. Ct. 2206, 2216–17 (2018).

163. United States v. Maclin, 393 F. Supp. 3d 701, 707–08 (N.D. Ohio 2019).

164. United States v. Schaefer, No. 3:17-cr-00400-HZ, 2019 WL 267711, at *5 (D. Or. Jan. 17, 2019).

165. *See* United States v. Monroe, 350 F. Supp. 3d 43, 49 (D.R.I. 2018); *see also* United States v. Contreras, 905 F.3d 853, 857 (5th Cir. 2018).

166. *Monroe*, 350 F. Supp. 3d at 49.

167. United States v. McCutchin, No. CR-17-01517-001-TUC-JAS, 2019 WL 1075544, at *3 (D. Ariz. Mar. 7, 2019).

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

169. United States v. Jenkins, No. 18-cr-00181, 2019 WL 1568154, at *4–5 (N.D. Ga. Apr. 11, 2019).

170. *Carpenter*, 138 S. Ct. at 2218.

171. *See supra* text accompanying notes 142–44.

connections for six months may not rise to "near perfect surveillance"[172] as required by *Carpenter*, but it certainly provides enough intrusion into a private life that it should warrant Fourth Amendment protection.

Third, the opinion specifies that it is not making any determination regarding real-time CSLI and tower dumps, which has been interpreted in widely varying ways, leading to some confusing decisions. For example, the Kansas District Court held that real-time CSLI only reveals an individual's location at that very moment of seizure.[173] Therefore, real-time CSLI does not meet the threshold for location tracking established by *Carpenter* and is not entitled to any Fourth Amendment protection. However, the Texas Criminal Court of Appeals also held that, while an individual does not have a reasonable expectation of privacy in *short term*[174] real-time CSLI tracking, they *may* have a reasonable expectation of privacy in "longer-term" tracking *if* it reveals the "privacies of life."[175] These two cases illustrate how the narrowness of *Carpenter* leads to inconsistent and vague holdings. Additionally, it is not intuitive how *Carpenter* can apply to historical CSLI but not real-time CSLI since the technology is identical.

These three criticisms of *Carpenter* are significant in illuminating the shortfalls of the opinion. In conclusion, it is difficult for lower courts to apply the framework outside the context of historical CSLI.

VI. SUGGESTIONS FOR FUTURE INTERPRETATION

The issues the Court focused on in *Carpenter* are the comprehensiveness of location tracking and the third-party doctrine. Two suggestions can be made with regard to providing better protection from government intrusion and surveillance.

The first is to approach location tracking from a broader perspective. A broader application is not barred by the language of the *Carpenter* opinion, because it stated that it was only discussing historical CSLI and expressly not deciding any other types of technology,[176] leaving other technology open for interpretation. It is possible to expose "familial, political, professional, religious, and sexual associations"[177] and the

172. *Carpenter*, 138 S. Ct. at 2218.

173. United States v. Thompson, No. 13-40060-10-DDC, 2019 WL 3412304, at *7 (D. Kan. July 29, 2019).

174. *Sims v. State* involved "less than three hours of real time CSLI" tracking. 569 S.W.3d 634, 646 (Tex. Crim. App. 2019).

175. *Id.* (quoting *Carpenter*, 138 S. Ct. at 2217).

176. 138 S. Ct. at 2220.

177. *Id.* at 2217 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (internal quotations omitted)).

"privacies of life"[178] without engaging in "near perfect surveillance."[179] Furthermore, if the challenged technology in a case can be described in the same way as the Court in *Carpenter* described CSLI's "deeply revealing nature . . . , its depth, breadth, and comprehensive reach and the inescapable and automatic nature of its collection,"[180] it should be protected by the Fourth Amendment under this broader application.

IP addresses are another example of technology where this broader application would be appropriate. Since an IP address is a unique identification for a device[181] that creates an automatic record of each location a device accesses the internet,[182] it is undoubtedly possible to easily infer "familial, political, professional, religious, and sexual associations"[183] by examining these location records. These records can be "deeply revealing . . . comprehensive . . . and . . . inescapable"[184] because IP addresses automatically record every single location a device accesses the internet, and it is not even possible to use the internet without an IP address.

Even though an IP address requires the affirmative act of accessing the internet, unlike CSLI, this is not enough to defeat the support for a broader application of *Carpenter*. The Supreme Court emphasized that cell phones are "indispensable to participation in modern society,"[185] which signals an understanding that the affirmative act requirement is not strictly construed.[186] Since it is not possible to use the internet without creating an IP address, and they are created automatically without any act beyond the cell phone owner using the phone as they

178. *Id.* at 2214 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

179. *Id.* at 2218.

180. *Id.* at 2223.

181. *What Is an IP Address?*, *supra* note 140.

182. United States v. Jenkins, No. 1:18-cr-00181, 2019 WL 1568145, at *4 (N.D. Ga. Apr. 11, 2019).

183. *Carpenter*, 138 S. Ct. at 2217 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (internal quotations omitted)).

184. *Id.* at 2223.

185. *Id.* at 2220.

186. In 1985, the Lifeline Program started to bring low-cost phone services to qualified individuals who were the recipients of assistance programs such as Medicaid. *Lifeline Program for Low-Income Customers*, FED. COMMC'NS COMM'N (Dec. 28, 2020), https://www.fcc.gov/general/lifeline-program-low-income-consumers. This program was modernized by an order issued by the Federal Communication Commission ("FCC") on March 31, 2016. *Id.* As part of the modernization, all phones provided to eligible consumers must be WiFi enabled as of December 1, 2016. *Id.* The existence of this requirement further supports the majority's argument that cell phones are such an essential part of modern society because there are assistance programs to increase access to them.

normally would,[187] it follows that IP addresses should be considered "deeply revealing . . . comprehensive . . . inescapable . . . automatic [in] nature . . ."[188] and deserving of Fourth Amendment protection.

For example, this interpretation would have changed the outcome in *United States v. Jenkins*, where the government obtained an incredible six months of IP addresses without a warrant.[189] Those six months of records reveal every location where a defendant sent an email, read an online article, or checked the score of a sports game. This is certainly comprehensive enough to meet the criteria for Fourth Amendment protection with a broader application. Moreover, this application would create a more consistent manner in which courts are dealing with IP addresses, as opposed to the current situation where some courts hold that IP addresses do not sufficiently track one's location[190] and other courts hold that the third-party doctrine applies to IP addresses.[191]

This broader application would also provide for the strong probability of Fourth Amendment protection for real-time CSLI tracking for a long period of time. It is simply not rational that real-time CSLI is not protected in the same way historical CSLI is protected, and this leads to varying and inconsistent opinions as discussed in Part III.

The second suggestion concerns the complicated relationship between the third-party doctrine and burgeoning twenty first century technology.[192] The *Carpenter* decision described the characteristics of CSLI that trigger protection as its "deeply revealing nature . . . , its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection."[193] These criteria should be used as the metric for determining whether the third-party doctrine applies to a certain type of challenged technology.

The courts' disposition of challenges regarding the acquisition of IP addresses would change with these criteria. Since IP addresses create a record of each location at which a device accesses the internet,[194] this is

187. The affirmative act of things such as an eBay transaction or paying an online bill is different from that of an IP address because those acts are fully voluntary and affirmative and they do not involve any additional automatic data collection, unlike IP addresses.

188. *Carpenter*, 138 S. Ct. at 2223.

189. *See supra* text accompanying notes 141–44.

190. United States v. Monroe, 350 F. Supp. 3d 43, 49 (D.R.I. 2018).

191. United States v. McCutchin, No. CR-17-01517-001-TUC-JAS, 2019 WL 1075544, at *2 (D. Ariz. Mar. 7, 2019); United States v. Contreras, 905 F.3d 853, 857 (5th Cir. 2018).

192. See *Carpenter*, 138 S. Ct. at 2261–72 (Gorsuch, J., dissenting) for a discussion regarding the weak Fourth Amendment protection created by putting the third-party doctrine on "life support" as it relates to modern technology.

193. *Id.* at 2223 (majority opinion).

194. *What Is an IP Address?*, *supra* note 140.

both "inescapable" and "automatic [in] nature."[195] The understandable counterargument to this would be that one does not have to have a cell phone or use it to access the internet. However, there are not many realistic alternatives to cell phone use. Even the Court in *Carpenter* acknowledged that cell phones are "almost a 'feature of human anatomy'"[196] and "faithfully follows its owner."[197] Continuing to apply the third-party doctrine despite this acknowledgement is simply not logical. IP addresses meet the criteria enumerated by the Court and should be afforded the same protection as historical CSLI.

Similarly, the third-party doctrine should not apply to cell tower dumps. Cell tower dumps are collected from the same cell sites as CSLI,[198] meaning they, too, are "deeply revealing," "inescapable," and "automatic" in nature.[199]

The shift in application for the third-party doctrine would provide a significant decrease in the information available without a warrant. This represents the shield from government intrusion the Founders intended the Fourth Amendment to provide, as Justice Brandeis illuminated so poignantly in his famous *Olmstead* dissent.[200]

VII. CONCLUSION

Cell phones provide a wide array of functions beyond calls and texting,[201] resulting in the potential for a comprehensive collection of data that can reveal "familial, political, professional, religious, and sexual associations."[202] This includes starting a vehicle—revealing the location of one's car every time this feature is used, monitoring a heart rate—revealing health information, and playing television shows—revealing a range of potential associations, including political, religious, and sexual.[203]

In the 2020—21 Coronavirus ("COVID-19") pandemic, cell phones also represent a potential avenue for contact tracing to try to slow the

195. *Carpenter*, 138 S. Ct. at 2223.
196. *Id.* at 2218 (quoting Riley v. California, 573 U.S. 373, 385 (2014)).
197. *Id.*
198. Tower dumps are "a download of information on all the devices that connected to a particular cell site during a particular interval." *Id.* at 2220.
199. *Id.* at 2223.
200. *See* Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).
201. *See* Crow, *supra* note 117.
202. *Carpenter*, 138 S. Ct. at 2217 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).
203. *See* Crow, *supra* note 117.

spread of the virus through our country.[204] Google and Apple collaborated to create a cell phone application that tracks an individual through Bluetooth.[205] This records the phone's proximity to another and if the owner tests positive for COVID-19, the records are used to send out alerts to those that have been within a certain Bluetooth vicinity to the patient.[206] These records have been described by the American Civil Liberties Union as "highly revealing" because they expose an individual's associates.[207] Although contact tracing applications are voluntary for now, if they become mandatory, the *Carpenter* opinion as it stands will do nothing to provide cell phone privacy because it does not protect Bluetooth technology. A broader application of *Carpenter*, however, would be useful because its current application risks exposing "familial, political, professional, religious, and sexual associations"[208] and is "deeply revealing [in] nature," deep, broad, and comprehensive, and its collection is "inescapable and automatic [in] nature.[209] Such information, therefore, should be subject to Fourth Amendment protection.

Consumers are seeking cell phones that provide better privacy from the constant tracking[210] and products that prevent the transmission of the constant tracking and defend one's privacy.[211] These products demonstrate the public yearning for more privacy as technology expands.

Unfortunately, *Carpenter* falls far short of the expectation that it would create more cell phone privacy. The failure to change the third-party doctrine as it relates to modern technology and the high threshold for tracking one's location to be considered a search make it exceedingly difficult to apply Fourth Amendment protection to anything other than historical CSLI. Until the Supreme Court of the United States grants certiorari to another case dealing with warrantless collection of cell phone technology, CSLI will remain unprotected by the shield of the Fourth Amendment.

204. Jennifer Stisa Granick, *Apple and Google Announced a Coronavirus Tracking System. How Worried Should We Be?*, ACLU (Apr. 16, 2020), https://www.aclu.org/news/privacy-technology/apple-and-google-announced-a-coronavirus-tracking-system-how-worried-should-we-be/.

205. *Id.*

206. *Id.*

207. *Id.*

208. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

209. *Id.* at 2223.

210. *See* Jon Knight, *The 4 Best Phones for Privacy and Security in 2020*, GADGET HACKS (Mar. 12, 2020, 12:04 PM), https://smartphones.gadgethacks.com/how-to/5-best-phones-for-privacy-security-0176106/.

211. *See generally* PRIVACYCASE, https://www.privacycase.com/ (last visited Jan. 18, 2020).