University of Arkansas at Little Rock Law Review

Volume 43 | Issue 4 Article 3

2022

Criminal Procedure—Technology in the Modern Era: The Implications of Carpenter v. United States and the Limits of the Third-Party Doctrine as to Cell Phone Data Gathered Through Real-Time Tracking, Stingrays, and Cell Tower Dumps

Deepali Lal

CRIMINAL PROCEDURE—TECHNOLOGY IN THE MODERN ERA: THE IMPLICATIONS OF *CARPENTER V. UNITED STATES* AND THE LIMITS OF THE THIRD-PARTY DOCTRINE AS TO CELL PHONE DATA GATHERED THROUGH REAL-TIME TRACKING, STINGRAYS, AND CELL TOWER DUMPS

I. INTRODUCTION

Cell phones are ubiquitous. In the United States, over ninety percent of the population has a cell phone, and over seventy-five percent of people have smartphones.[1] Today, almost anything can be done with the swipe of a fingertip, even planning, and executing a series of robberies.[2] Consider a person using a cell phone to help his or her accomplices steal phones. To put the leader in jail, the government then tries to obtain cell phone records, containing call details and all the towers the cell phones connected to when the individual used his phone.[3] Authorities can use this information to determine a suspect's proximity to the location of a robbery.[4] However, cell-site location information (CSLI) is not captured occasionally for the interdiction of crime; it is continuously gathered from every phone that connects to every tower—even yours.[5]

Are you providing this information of your own volition when you are using a cell phone?[6] What about when your phone is merely powered on and traveling in your pocket? This is exactly what happened in *Carpenter v. United States*.[7] The advancement of technology has benefitted nearly every sector of society; however, it has unintentionally become a threat to individual privacy.[8] Even though the framers of the Fourth Amendment could not predict the advancements of modern technology, the Fourth Amendment's protection from warrantless searches has expanded into the digital world.[9]

---

1. Joe Mitchell & Shawn Webb, *Is Big Brother Watching Us: The Evolving State of the Law on Cell Phone, Digital Evidence, and Privacy*, 88 HENNEPIN LAW. 14, 16 (2019).
2. *See* Carpenter v. United States, 138 S. Ct. 2206, 2209 (2018).
3. *Id.* at 2212–13.
4. *Id.* at 2210.
5. *Id.* at 2211.
6. Laura K. Donahue*, Functional Equivalence and Residual Rights Post*-Carpenter*: Framing a Test Consistent with Precedent and Original Meaning*, SUP. CT. REV. 347, 384 (2018).
7. 138 S. Ct. 2206 (2018).
8. Cal Cumpstone, Note, *Game of Phones: The Fourth Amendment Implications of Real-Time Cell Phone Tracking,* 65 CLEV. ST. L. REV. 75, 76 (2016).
9. Andrew Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 566 (2017).

Carpenter v. United States exemplifies the increasing need to consider how technological advances impact constitutional rights.[10] Before *Carpenter*, the Court had cultivated what had become known as the third-party doctrine which established that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[11] However, the *Carpenter* Court held that an individual has a reasonable expectation of privacy in his or her historical CSLI, and that the government must obtain a warrant before accessing detailed location information.[12] In so ruling, the Court declined to "extend" the third-party doctrine, which had been used for over forty years.[13] Instead, the Court restricted the scope of the third-party doctrine as most commentators and courts previously understood it.[14]

Despite the monumental implications of *Carpenter*, the actual holding was narrow; the Court did not decide the implications of government surveillance techniques like real-time tracking and web-browsing.[15] What makes real-time tracking intrusive is that police officers can continuously monitor individuals' cell phones without the individuals noticing.[16]

This note argues that the Supreme Court should extend the holding of *Carpenter v. United States* to real-time tracking, stingrays,[17] and cell tower dumps[18] because they are intrusive and provide intimate details of people's lives that would otherwise not be known. Part II of this note provides background information on *Carpenter v. United States* and analyzes the narrow ruling's impact on an individual's expectation of privacy. Part III analyzes the constitutional implications of *Carpenter* and argues that the Supreme Court should apply its holding to real-time tracking, stingrays, and cell tower dumps because these technologies are just as invasive as CSLI and provide intimate details of an individual's life that may not otherwise be known. Because *Carpenter* has a narrow ruling, Part IV argues that Congress must enact electronic "exhaustion" requirements for surveillance to

10. *Carpenter*, 138 S. Ct. at 2224 (Kennedy, J., dissenting).

11. *Id*. at 2216 (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).

12. *Id.* at 2221.

13. Greg Nojeim, *Wider Implications of* Carpenter v. United States, 2 INT'L J. DATA PROTECTION OFFICER, PRIVACY OFFICER & PRIVACY COUNS. 8, 8 (2018).

14. Susan Freiwald & Stephen W. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 212–14 (2018).

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

16. Cumpstone, *supra* note 8, at 77.

17. Howard W. Cox, *Stingray Technology and Reasonable Expectations of Privacy in the Internet of Everything*, 17 FED. SOC'Y REV. 29, 29–30 (Mar. 31, 2016), http://www.fedsoc.org/publications/detail/stingray-technology-and-reasonable-expectations-of-privacy-in-the-internet-of-everything (describing stingrays as cell-site simulators. Stingrays are used to determine and track cell phones criminals use when they engage in criminal activity. They pose as cell towers and can help law enforcement pinpoint the cell phone the suspect uses.).

18. *Carpenter*, 138 S. Ct. at 2220 (defining "tower dumps" as "a download of information on all the devices that connected to a particular cell site during a particular interval.").

prevent a broad invasion of privacy. Enacting exhaustion requirements[19] will protect people from the invasion of their reasonable expectation of privacy and will establish that law enforcement may only track cellphones when needed; it will not be a first resort. Thus, law enforcement should initially engage in less invasive investigative procedures.

II. BACKGROUND

The Fourth Amendment protects people from unreasonable searches and seizures. As technology is rapidly changing, the law has evolved. This section will provide a brief historical overview of Fourth Amendment jurisprudence pre-*Carpenter* and analyze *Carpenter*'s holding.

A. Historical Overview—Pre-*Carpenter*

Much of the Supreme Court's Fourth Amendment jurisprudence in the last century has reflected the challenges of applying the Fourth Amendment to newly developed technology; in the decade before *Carpenter*, this caused the Court to modify its interpretation of the Fourth Amendment twice to apply to modern technology.[20] As a result, the government has been required to obtain a search warrant before it goes through the contents of a cell phone when it is seized during a search incident to arrest or when it attaches a GPS tracker to follow the movement of a vehicle.[21]

The Fourth Amendment protects privacy from unreasonable government intrusion.[22] Historically, courts have held that a search can occur within the meaning of the Fourth Amendment in one of the three following ways: (1) physical trespass;[23] (2) invasion of an individual's reasonable expectation of privacy;[24] or (3) virtual trespass.[25] In response to new concerns

19. Jake Laperruque, *Congress Should Place More Limits on Cellphone Location Tracking After* Carpenter*,* JUST SECURITY (March 23, 2018), https://www.justsecurity.org/54231/probable-cause-electronic-exhaustion-limits-location-tracking-carpenter/ (highlighting there are no exhaustion requirements currently for the rules of gathering location data similar to the Wiretap Act, "which governs warrants for intercepting communications").

20. Evan Kaminker, *Location Tracking and Digital Data: Can Carpenter Build a Stable Privacy Doctrine?*, SUP. CT. REV. 411, 411 (2018).

21. Riley v. California, 573 U.S. 373, 373 (2014); *See Jones*, 565 U.S. at 400.

22. U.S. CONST. amend. IV. ("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.").

23. Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding that a search occurs when the government physically occupies a citizen's private property for the purposes of obtaining information).

24. Katz v. United States, 389 U.S. 347, 358–59 (1967) (holding whether a search occurs under a *Katz* analysis depends on whether that person actually exhibited a subjective

created by a world of rapidly evolving technological advancements, *Olmstead v. United States* was the first case that examined the "implications" of technology under the Fourth Amendment.[26] The *Olmstead* Court declined to extend the protection of the Fourth Amendment to wiretapped telephone lines located outside Olmstead's property.[27] The Court held that the government did not conduct a search or seizure because the agents tapped Olmstead's phone lines "without any trespass upon [his] property."[28] The *Olmstead* Court set forth the trespass-doctrine which triggers Fourth Amendment protection when an officer makes "an actual invasion of [the defendant's] house 'or curtilage'[29] for the purpose of making a seizure."[30]

In the 1980s, the Supreme Court established a constitutional framework for tracking devices in *United States v. Knotts*[31] and *United States v. Karo*.[32] In the 1990s, Congress enacted statutes that recognized that customers had some right to privacy in cell phone tracking data, though Congress did not address the legal standard authorizing this type of surveillance.[33] The reasonable expectation of privacy test was established in *Katz v. United States*, in Justice Harlan's concurrence.[34] In *Katz*, the Court held that when law enforcement agents placed a listening device near a public phone booth to eavesdrop and record the defendant's conversation,[35] it was an infringement on the defendant's reasonable expectation of privacy. Once the defendant

---

expectation that the object of the alleged search was private, and whether society is prepared to recognize that expectation as reasonable).

25. Kyllo v. United States, 533 U.S. 27, 34 (2001) (holding a virtual trespass occurs when the government uses sense-enhancing technology that is not in general public use to obtain information regarding the interior of a home that could not otherwise have been obtained without "physical intrusion into a constitutionally protected area").

26. Cumpstone, *supra* note 8, at 78.

27. *Olmstead*, 277 U.S. at 466.

28. *Id.* at 457.

29. Oliver v. United States, 466 U.S. 170, 180 (1984) (defining curtilage at common law as "the area to which extends the intimate activity associated with the sanctity of a person's home and the privacies of life" (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

30. *Olmstead*, 277 U.S. at 466.

31. 460 U.S. 276, 281 (1983) (holding that an individual has no reasonable expectation of privacy in his or her movements on public roads and highways).

32. 468 U.S. 705, 716 (1984) (holding that a search occurs within the meaning of the Fourth Amendment when the government agents use electronic surveillance to obtain information about the interior of a private residence that would otherwise not be available through plain view beyond the curtilage of the residence).

33. Freiwald & Smith, *supra* note 14, at 206.

34. Aaron L. Dalton, *Carpenter v. United States: A New Era for Protecting Data Generated on Personal Technology, or a Mere Caveat?*, 20 N.C. J. L. & TECH. ON. 1, 11 (2018); *see also Katz,* 389 U.S. at 361 (holding that under Justice Harlan's test a person must (1) have "exhibited an actual (subjective) expectation of privacy," and (2) society must be prepared to deem that expectation reasonable).

35. *Katz*, 389 U.S. at 348.

entered the telephone booth, shut the door, and paid the toll he had a reasonable expectation that his conversation would not be recorded.[36]

On the other hand, *United States v. Miller* created the third-party doctrine, which limited *Katz*, holding that a person has no Fourth Amendment protection against the government obtaining information that he or she has voluntarily conveyed to a third party.[37] The *Miller* Court found no reasonable expectation of privacy in an individual's bank records that the account holder had voluntarily conveyed to the bank and were also the bank's own business records.[38] *Smith v. Maryland* extended the third-party doctrine to dialed phone numbers.[39] In *Smith*, a telephone company installed a pen register to observe outgoing calls from the defendant's phone.[40] Although the pen register did not record the contents of the conversation, it recorded the telephone numbers dialed.[41] Smith had no expectation of privacy in the dialed telephone numbers because it is common for companies to store numbers.[42] Thus, society would not recognize Smith's expectation of privacy as reasonable because he had voluntarily exposed this information to a third party.[43]

In *United States v. Jones*, instead of relying on the *Katz* test, the Court revived the trespass doctrine.[44] In *Jones*, the government attached a GPS tracking device to the undercarriage of a vehicle and tracked an individual.[45] Even though the data obtained from the device consisted of 2,000 pages of data during the course of four weeks, the majority opinion never addressed whether the "length and comprehensiveness of surveillance" violated Jones' reasonable expectation of privacy.[46] Instead the majority found that the government's action was a "physical intrusion of property for the purpose of obtaining information" and was thus a search within the meaning of the Fourth Amendment.[47] *Jones* did not replace the reasonable expectation of privacy test, which originated in *Katz*.[48] Instead, *Jones* relied on the trespass doctrine; it held that the *Katz* test had supplemented, rather than replaced,

36. *Id.* at 361 (Harlan, J., concurring).
37. *See* United States v. Miller, 425 U.S. 435 (1976).
38. Dalton, *supra* note 34, at 11.
39. Smith v. Maryland, 442 U.S. 735, 741–43 (1979).
40. *Id.*
41. *Id.* at 741.
42. *Id.*
43. *Id.* at 743–44.
44. Cumpstone, *supra* note 8, at 81. *See* United States v. Jones, 565 U.S. 400 (2018).
45. *Jones*, 565 U.S. at 413.
46. Cumpstone, *supra* note 8, at 82.
47. *Id.*
48. *Jones*, 565 U.S. at 406.

the trespass doctrine from *Olmstead*.[49] Before *Jones*, it was long considered that the *Katz* test had replaced the trespass doctrine from *Olmstead*.[50]

CSLI came into the limelight in 2008 when the U.S. District Court for the Western District of Pennsylvania ruled that the government could not obtain CSLI under a Section 2703 D order[51] because the Electronic Privacy Communications Act's text and legislative history did not distinguish between real-time location information and historical CSLI.[52] Conversely, the Fifth Circuit held the release of CSLI did not violate the Fourth Amendment because the CSLI records were business records conveyed to a third-party by the individual; therefore, the individual had no reasonable expectation of privacy against the government obtaining the records.[53] This ushered in a long-standing disagreement among the courts focusing on whether cell phone users "voluntarily convey" location information to telephone carriers and whether CSLI is entirely metadata.[54] However, the Supreme Court's 2018 landmark decision in *Carpenter v. United States* altered the discussion once again.

B. Background on *Carpenter v. United States*

In *Carpenter v. United States,* the government obtained cell phone records of suspects in a robbery, which provided CSLI information of the suspects' activities. The Supreme Court held that cell-site location information is protected under the Fourth Amendment.

---

49. *Id.* at 409.

50. *Id.* at 406.

51. 18 U.S.C. § 2703(d) (describing a D order forces an internet service provider to provide detailed electronic records about a customer such as Internet Protocol addresses and addresses of people who the customer exchanged emails with).

52. *In re* United States for an Ord. Directing Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 601 (W.D. Pa. 2008); *see also* Freiwald & Smith, *supra* note 14, at 206.

53. *In re* United States for an Ord. Directing Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d at 601.

54. Peter C. Ormerod & Lawrence J. Trautman, *A Descriptive Analysis of the Fourth Amendment and the Third-Party Doctrine in the Digital Age*, 28 ALB. L.J. SCI. & TECH. 73, 133–34 (2018); *see also* Orin Kerr, *Relative vs. Absolute Approaches to the Content/Metadata Line*, LAWFARE BLOG (Aug. 25, 2016, 4:18 P.M), https://www.lawfareblog.com/relative-vs-absolute-approaches-contentmetadata-line (defining the substance of the message as contents and the information of the message as metadata. Contents receive a higher level of protection compared to metadata. When talking about a phone call, the contents are the actual sounds on the call, whereas the metadata are the numbers dialed and times of the phone call.).

1. Facts

In 2011, the police arrested four suspects for robbing a series of T-Mobile and Radio Shack Stores in Detroit, Michigan.[55] One of the suspects conceded that over the course of four months the group robbed nine stores in Michigan and Ohio; he also gave the FBI phone numbers of some of the accomplices.[56] Prosecutors then applied for an order under the Stored Communications Act to obtain the suspects' cell records.[57] The Stored Communications Act permits the government to demand the disclosure of specific telecommunication records when law enforcement has shown reasonable and articulable facts that the records being requested are "relevant and material to an ongoing criminal investigation."[58] Metro PCS and Sprint, Carpenter's wireless carriers, were ordered to disclose Carpenter's CSLI records during the four months.[59]

CSLI is a "time-stamped location" generated when a phone attaches to a cell site.[60] The magistrate judge issued two orders; the first order sought CSLI records for 152 days of calls but yielded records of 127 days, and the second-order sought seven days of CSLI records from Sprint, but the government obtained only two days of records when Carpenter's phone was in Ohio on "roaming."[61] In total, the government received 12,898 location points that documented Carpenter's movements, and the information showed that Carpenter's cell phone was near four of the robbery locations when the robberies occurred.[62] Carpenter was charged with six counts of robbery and six counts of carrying a firearm.[63]

Before trial, Carpenter moved to suppress the CSLI provided by the wireless carriers.[64] He argued that the collection of data was a search under the meaning of the Fourth Amendment and the police were required to obtain a warrant based on probable cause.[65] At trial, FBI agent Christopher Hess presented maps that showed Carpenter's phone was near four of the charged robberies; the location records confirmed Carpenter was present "at the exact time of the robbery," so the jury convicted him on all except one of the firearm counts and sentenced to more than 100 years in prison.[66]

55. Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).
56. *Id.*
57. *Id.*
58. 18 U.S.C. § 2703(d).
59. *Carpenter*, 138 S. Ct. at 2212.
60. *Id.* at 2211.
61. *Id.* at 2212.
62. *Id.* at 2212–13.
63. *Id.* at 2212.
64. *Id.*
65. *Carpenter*, 138 S. Ct. at 2212.
66. *Id.* at 2212–13.

2. Holding/Reasoning

The District Court denied Carpenter's motion to suppress the evidence, in which he argued that obtaining his records was a violation of the Fourth Amendment because the Government acquired the records without a warrant.[67] The Sixth Circuit reasoned that Carpenter did not have a reasonable expectation of privacy because he voluntarily disclosed his location information to his cell phone carrier.[68] Yet, the *Carpenter* Court retreated from the third-party doctrine.[69] Instead, the Supreme Court created a new balancing test that weighs the reasonable expectation of privacy against whether the information was voluntarily disclosed to a third-party.[70] The first step is to determine if there is a "reduced" expectation of privacy.[71] To determine this, a court must consider the following: the "nature" of the certain documents sought and if there is a "legitimate expectation of privacy" regarding the details. [72] Pervasiveness is another factor courts may use to determine if there is a "reasonable" or reduced expectation of privacy.[73] Compiling detailed data from a person's day, week, or month provides a "detailed chronicle of a person's presence" and is sufficiently pervasive that the person would have a reasonable expectation of privacy in the chronicled information.[74]

Another factor is the individual's voluntary exposure. The information must be "truly 'shared; if the individual has a choice, then the information is truly shared.'"[75] If the only choice is to consent to disclosure or disconnect the phone, there is no real choice, and the disclosure is not voluntary.[76] Carpenter did not voluntarily and knowingly disclose his CSLI data with his cellphone provider because CSLI was generated without fail by the service provider; he would have had to disconnect his cell phone in order to avoid sharing his CSLI information entirely.[77] In *Carpenter*, the Court found it important that cell phones are "indispensable to participation in modern society."[78] At this stage, the Court evaluates the assumption of risk after an

67. *Id.* at 2212.
68. *Id.* at 2213.
69. *See id.* at 2220 (holding that the third-party doctrine does not apply to CSLI).
70. *See generally id*; *see also* Mary-Kathryn Takeuchi, Note, *A New Third-Party Doctrine: The Telephone Metadata Program and Carpenter v. United States*, 94 NOTRE DAME L. REV. 2243, 2244 (2019).
71. *Carpenter*, 138 S. Ct. at 2219.
72. *Id.*
73. *Id.* at 2220.
74. *Id.* at 2219–20.
75. *See id*. at 2220; Takeuchi, *supra* note 70, at 2253.
76. *Id*.
77. Freiwald & Smith, *supra* note 14, at 225.
78. *Carpenter*, 138 S. Ct. at 2220.

individual makes an affirmative act.[79] Calls, emails, and texts all generate CSLI information; thus, there is no way to stop sending this information other than to disconnect the phone from a network.[80]

Accordingly, the Court found that cell phone users do not voluntarily assume the risk of sharing comprehensive records of their physical movements.[81] The Court held that Carpenter had a reasonable expectation of privacy in the information, meaning there was a search under the Fourth Amendment.[82] Furthermore, the Court held that the search violated Carpenter's Fourth Amendment rights because the circumstances in the case required a warrant to make the search reasonable.[83]

Carpenter reiterated that the purpose of the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by government officials."[84] Several states ratified the Fourth Amendment in response to the general warrants and writs of assistance that gave British officers the authority to forage through homes to search for evidence of a crime.[85] As technology advances, most personal information is no longer stored in the traditional way of physical papers; instead, people store their information on digital devices or sometimes in the "cloud," something the Framers of the Fourth Amendment did not anticipate in 1791.[86] However, the doctrine does not completely bar expectation of privacy, because there are limits such as physical space, physical items that are possessed by third parties temporarily,[87] and now CSLI.[88]

3. Dissenting Opinions

Justices Kennedy, Thomas, Alito, and Gorsuch dissented. Justice Kennedy argued that consumers do not have a reasonable expectation of privacy because people do not control these records.[89] He observed that the majority's test suggested that Fourth Amendment protections applied when private

79. Takeuchi, *supra* note 70, at 2253.
80. *Carpenter*, 138 S. Ct. at 2220.
81. *Id.*
82. *See id.* at 2219.
83. *Id.* at 2221.
84. *Id.* at 2213.
85. Riley v. California, 573 U.S. 373, 403 (2014).
86. Kaitlin D. Corey, *How Far Will the Third Party Doctrine Extend*, 51 MD. B.J. 14, 15 (2018).
87. Ormerod & Trautman, *supra* note 54, at 114 (discussing three limitations on the third-party doctrine are "that people retain a reasonable expectation of privacy in physical spaces owned by a third party, in physical things left with another party, and in at least one type of information conveyed to a third party").
88. *See Carpenter*, 138 S. Ct. 2206 (2018).
89. *Id.* at 2224 (Kennedy, J., dissenting).

interests weigh more heavily than the third-party disclosure.[90] Justice Kennedy noted that this balancing test departs from the bright-line rule of the third-party doctrine.[91]

Justice Thomas emphasized that instead of focusing on whether a search occurred, the focus should be "*whose* property was searched."[92] He argued that the records did not belong to Carpenter because he neither generated nor controlled them;[93] the records belonged to MetroPCS and Sprint.[94] Justice Alito argued that probable cause should not be required for mandatory rendering of records but should be required for an actual search on private property.[95] Under Alito's interpretation, any personal information that could be found on paper could be subpoenaed.[96] Justice Gorsuch's dissent resembles a concurring opinion more than a dissent because he rejected the third-party doctrine.[97] He endorsed the "traditional approach" to interpreting the Fourth Amendment, which asks "if a house, paper, or effect was *yours* under the law,"[98] and he suggested his willingness to consider the CSLI to be Carpenter's papers or effects, except that Carpenter had forfeited the argument by failing to preserve it.[99]

4. A qualitative and quantitative test emerged from Carpenter

The *Carpenter* Court applied *Katz*'s reasonable expectation of privacy test in addition to a more favorable multi-factor test.[100] This is a fundamental shift in the jurisprudence of the Fourth Amendment because it traditionally focused on law enforcement's conduct while obtaining this kind of information.[101] The Court shifted its focus to the type of information the government seeks. Under *Carpenter*, in any instance the government obtains a court order for detailed information about individuals that is not available to

90. *Id.* at 2232.
91. Takeuchi, *supra* note 70, at 2250.
92. *Carpenter*, 138 S. Ct. at 2235 (Thomas, J., dissenting).
93. *Id.*
94. *Id.*
95. *Id.* at 2221.
96. *Id.* at 2222.
97. Ashley Baker, *Gorsuch's dissent in 'Carpenter' case has implications for the future of privacy*, THE HILL (June 26, 2018, 2:45 PM), https://thehill.com/opinion/cybersecurity/394215-gorsuchs-dissent-in-carpenter-case-has-implications-for-the-future-of (last visited Sept. 22, 2019).
98. *Carpenter*, 138 S. Ct. at 2268 (Gorsuch, J., dissenting).
99. *Id.* at 2272.
100. *Id.* at 2223.
101. United States v. Jacobsen, 466 U.S. 109, 113 (1984) (stating that the "reasonableness" requirement of the Fourth Amendment has been consistently construed to regulate governmental action); *Katz*, 389 U.S. at 353 (examining law enforcement's actions to determine whether the Fourth Amendment was implicated).

the public, the judge will carry out a qualitative and quantitative assessment of the information.[102] The assessment consists of two questions.[103] First, does the individual whose detailed information is obtained have a reasonable expectation of privacy?[104] And second, even if a third party collects and maintains that information, does the third-party doctrine apply?[105]

The *Carpenter* Court implemented a three-factor test that should be used to evaluate information: (1) its "deeply revealing nature" (2) its "depth, breadth, and comprehensive reach," and (3) whether it "results from an inescapable and automatic form of data collection."[106] The importance of the deeply revealing nature of the information was developed by the Court in *United States v. Jones* and *Riley v. California.*[107] Under observation, an individual's information is protected only if it is deeply revealing.[108] The Court found time-stamped data is similar to GPS information.[109] It can provide private and undisclosed traits about a person such as "familial, political, professional, religious and sexual associations."[110] Arguably, the deeply revealing nature is the most important factor because the Court held that CSLI "hold[s] for many Americans the 'privacies for life.'"[111]

"Depth" refers to the detail and precision of the facts.[112] "Breadth" refers to how often data is collected and the amount of time over which it has been collected; "comprehensive reach" refers to the number of people being tracked in a database.[113] The Court highlighted that CSLI contains "the whole of [a person's] physical movements"[114] and a "detailed chronicle of a person's physical presence."[115] Most wireless carriers store CSLI for five years;[116] it is information "compiled every day, every moment, over several years."[117] The database in *Carpenter* stored "an average of 101 data points every day" of Carpenter's location.[118] "[L]ocation information is continually logged for all of the 400 million devices in the United States—not just those

102. Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J. L. & TECH 357, 369 (2019).
103. *Id.*
104. *Id.*
105. *Id.* at 369–70.
106. *Carpenter*, 138 S. Ct. at 2223 (2018).
107. *Id.* at 2213; *see also Riley*, 573 U.S. at 414; *Jones*, 565 U.S. at 406.
108. Ohm, *supra* note 102, at 371.
109. *Carpenter*, 138 S. Ct. at 2217, 2213.
110. *Id.* at 2217 (quoting *Jones*, 565 U.S. at 415).
111. *Riley*, 573 U.S. at 403 (citing Boyd v. United States, 116 U.S. 616, 630 (1886)).
112. Ohm, *supra* note 102, at 372.
113. *Id.* at 372–73.
114. *Carpenter*, 138 S. Ct. at 2219.
115. *Id.* at 2220.
116. *Id.* at 2218.
117. *Id.* at 2220.
118. *Id.* at 2212.

belonging to persons who might happen to come under investigation—this newfound tracking capability runs against everyone."[119]

Lastly, as discussed above, the Court looks at the "inescapable and automatic nature" of how information is collected.[120] Because cell phones have become such a pervasive part of life, their use cannot be considered "voluntary" or "escapable,"[121] and the automatic nature of CSLI collection suggests no meaningful ability for the user to "opt-out."[122] If cell phone use is an inescapable part of today's society and the collection of data therefrom is automatic, the cell phone owner has no autonomy over the information. He cannot disclose information over which he has no control.[123]

Carpenter also suggests the rule of "technological equivalence."[124] If the police have the ability to gather information from technology that is the "modern-day equivalent" of activity that the Court has held to constitute a search within the meaning of the Fourth Amendment, then the *use* of that equivalent technology also constitutes a search within the meaning of the Fourth Amendment.[125]

The *Carpenter* Court shifts the relevant inquiry from how law enforcement obtains information to how *detailed* is the information that law enforcement obtains. It created a three-factor test that courts use to assess what type of information law enforcement seeks. The Court held that accessing a person's historical cell-site records of seven or more days violates a person's reasonable expectation of privacy, and thus is a search within the meaning of the Fourth Amendment.[126] If CSLI is considered a search, the courts should also consider real-time tracking, stingrays, and cell-tower dumps as searches within the meaning of the Fourth Amendment because they provide more intrusive information than CSLI.

---

119. *Id.* at 2218.

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

121. Brief for Petitioner, at 39–42, *Carpenter*, 138 S. Ct. 2206 (No. 16-402).

122. *Carpenter*, 138 S. Ct. at 2220 ("Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart 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.").

123. *See* Ohm, *supra* note 102, at 376.

124. *Id.* at 360.

125. *Carpenter*, 138 S. Ct. at 2230 (Kennedy, J., dissenting); Ohm, *supra* note 102, at 360.

126. *Id.* at 2266 (Gorsuch, J., dissenting).

III. CONSTITUTIONAL IMPLICATIONS WITH NEW AGE TECHNOLOGY

Today, new technology like real-time tracking, stingrays, and cell tower dumps allow law enforcement to access even more data through cellphones. Real-time tracking is more intrusive than CSLI and can pinpoint the precise location where a person is standing. It reveals detailed information about a person's life, such as phone calls and texts that a person receives. Conveyance of this information is not voluntary. Stingrays, on the other hand, are more invasive than CSLI. They can determine a person's location within six feet. Lastly, cell tower dumps are like a dragnet because they collect detailed information as to a particular area. Cell tower dumps provide information for an unknown number of phones over a short period. As of yet, courts have not settled on a standard approach to evaluating these new technologies under the Fourth Amendment. This section will provide an overview of these modern technologies and current treatment in the U.S.

A. Real-Time Tracking

Real-time tracking occurs when police ping a cell phone and force it to send a signal; this then creates real-time location information.[127] It is prospective collection of information.[128] In real-time tracking, law enforcement can track a person's location as it is occurring.[129] The *Carpenter* Court left open the issue of real-time tracking.[130] A bright-line rule has not been established to determine the amount of time the police must track a person's cell phone in real-time before an individual's reasonable expectation of privacy is violated.[131] Lower courts have held that in determining if an individual has a reasonable expectation of privacy in real-time records, the expectation must be resolved case-by-case.[132]

Distinguishing between long- and short-term surveillance is dangerous because it can result in "arbitrary and inequitable enforcement," which is what the court held in *Tracey v. Florida*.[133] The Florida Supreme Court has rejected an approach based on the length of time that police monitor a cell phone's location.[134] In *Tracey*, the court found that an individual has a rea-

127. Matter of an Application of the U.S.A. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 534 (D. Md. 2011).

128. Cumpstone, *supra* note 8, at 84.

129. Samantha G. Zimmer, *Cell Phone or Government Tracking Device: Protecting Cell Site Location Information with Probable Cause*, 56 DUQ. L. REV. 107, 111 (2018).

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

131. Sims v. State, 569 S.W.3d 634, 646 (Tex. Crim App. 2019).

132. *Id.*

133. Tracey v. State, 152 So. 3d 504, 521 (Fla. 2014).

134. *Id.* at 521.

sonable expectation of privacy in his or her real-time location information.[135] Furthermore, the court found that people use cell phones for countless purposes, such as banking, sending emails and texts, and scheduling.[136] The court noted that the Fourth Amendment protects the rights of United States citizens to be secure in their own homes.[137] However, the government cannot always anticipate that people carry cell phones on their persons or nearby, which could be in the home.[138] Additionally, since the Fourth Amendment requires a warrant to particularly describe the place being searched, without the government knowing precisely where the cell phone is, tracking the phone without a warrant is the equivalent to a general warrant.[139]

On the other hand, a New York court in *In re Smartphone Geolocation Data Application* held that individuals have no reasonable expectation of privacy in their real-time location.[140] The court held that prospective CSLI was covered under the third-party doctrine.[141] The court stated that a cell phone user is "well aware" that the cell phone tracks the location of the phone and that the user can turn off the phone to prevent it from sending location information.[142] Thus, a user waives any reasonable expectation of privacy because he or she voluntarily conveys this real-time information.[143]

A Texas court held that three hours of real-time tracking did not invade an individual's reasonable expectation of privacy.[144] In *Sims v. State*, the state charged Christian Sims with murder. Sims filed a motion to exclude the evidence of real-time location information used to trace his cell phone by "pinging" without the police having obtained a warrant.[145] The trial court and the appellate court both denied the motion, prompting Sims to appeal his case to the Court of Criminal Appeals of Texas.[146] The court considered *Carpenter* and concluded that the content of the CSLI records were not im-

135. *Id.* at 525.
136. *Id.* at 523.
137. *Id.* at 511.
138. *Id.* at 524.; Matthew DeVoy Jones, *Cell Phones Are Orwell's Telescreen: The Need for Fourth Amendment Protection in Real-Time Cell Phone Location Information*, 67 CLEV. ST. L. REV. 523, 541 (2019).
139. *Tracey*, 152 So. 3d at 524.
140. *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 147 (E.D.N.Y. 2013).
141. *Id.*
142. *Id.* at 138.
143. *Id.* at 146.
144. Sims v. State, 569 S.W.3d 634, 646 (Tex. Crim App. 2019).
145. *Id.* at 636.
146. *Id.* at 637.

portant; it instead looked at whether enough information was obtained to violate an individual's reasonable expectation of privacy.[147]

Courts considering information-gathering techniques comparable to CSLI have continued to disagree about real-time tracking. *Carpenter* and *Sims* suggest a spectrum of permissible time to track a cell phone. In *Carpenter*, the court concluded that 127 days of data collection was a search,[148] whereas in *Sims* the data collection was limited to three hours, and the court concluded a search did not occur.[149] *Carpenter* provides a timing standard—when the government accesses seven days of historical CSLI, it constitutes a Fourth Amendment search.[150] The Court declined to decide whether some shorter period might be permissible without implicating the Fourth Amendment.[151]

B. Stingrays

Cell site simulators are more commonly known as "stingrays."[152] Stingrays operate in a manner similar to cell sites by functioning as mock towers, interrupting cell phone signals and collecting information from phones.[153] When a stingray is used, the government obtains information not from a third party, but by intercepting a signal that a user originally intended to send to a carrier's cell-site tower.[154] The government does this surreptitiously.[155] Because a stingray acts like a cell tower, cell phones that are near the vicinity are compelled to connect to the stingray;[156] even phones that are not in use will be connected to the stingray.[157] The data that is collected can consist of the following: serial numbers of the cell phones, the cell phone num-

147. Benson Varghese, *Sims v. State: Can Police Obtain Real-Time Cell Site Location Without Warrant*, https://www.versustexas.com/criminal/sims-v-state/ (last visited Oct. 25, 2019).

148. *Carpenter*, 138 S. Ct. at 2212.

149. *Sims*, 569 S.W.3d at 646.

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

151. *Id.*

152. Hanni Fakhouri & Trevor Trimm, *Stingrays: The Biggest Threat to Cell Phone Privacy You Don't Know About,* ELECTRONIC FRONTIER FOUNDATION (Oct. 22, 2012), https://www.eff.org/deeplinks/2012/10/stingrays-biggest-unknown-technological-threat-cell-phone-privacy.

153. Cody Benway, *You Can Run, But You Can't Hide: Law Enforcement's Use of "Stingray" Cell Phone Trackers and the Fourth Amendment*, 42 S. ILL. U. L. J. 261, 265 (2018).

154. Fakhouri & Trimm, *supra* note 152.

155. State v. Sylvestre, 254 So. 3d 986, 991 (Fla. Dist. Ct. App. 2018).

156. *Id.*

157. Olivia Donaldson, *The StingRay is Exactly Why the 4th Amendment was Written*, FOUNDATION FOR ECONOMIC EDUCATION (Feb 13, 2017), https://fee.org/articles/the-stingray-is-exactly-why-the-4th-amendment-was-written/.

ber, date, and time of calls.[158] Stingrays transmit this information about every seven seconds when the phone is powered on.[159] Stingrays can make a tracked device automatically send text messages or call someone, without the owner of the cell phone having to do anything.[160] Once a suspect is discovered, law enforcement can pinpoint the location using real-time tracking.[161]

In some states, law enforcement is not required to have a warrant when using stingrays to spy on people who are engaged in suspicious criminal activity.[162] However, some lower courts have held that cell site simulators constitute a search within the meaning of the Fourth Amendment.[163] The Maryland Supreme court in *State v. Andrews* held that individuals have a reasonable expectation of privacy that their cell phones will not be tracked in real-time.[164] Therefore, the court held that law enforcement's use of a cell site simulator constitutes a search within the meaning of the Fourth Amendment.[165] Furthermore, the New York Supreme court in *People v. Gordon* held a warrant was required for the extensive use of a cell site simulator because it violates an individual's reasonable expectation of privacy.[166]

The Seventh Circuit was the first circuit to address the use of stingrays.[167] In *Patrick v. United States*, the court stated that a cell site simulator is similar to a pen register, which is not a search because it does not reveal the content of the call, only the making of the call and the number.[168] On the other hand, the Ninth Circuit has not decided whether using cell site simulators to locate cell phones in real time constitutes a search.[169]

---

158. Benway, *supra* note 153, at 265.

159. Christopher D. Browne, *Ill-Suited to the Digital Age: Problems with Emerging Judicial Perspectives on Warrantless Searches of Cell Site Location Information*, 6 NW. INTERDISC. L. REV. 57, 62 (2013) (describing that cell phones automatically connect to the closest tower to receive the strongest strength. Every seven seconds, a cell phone sends a ping to nearby towers).

160. *Id.*

161. Jenna Jonassen, *Stingrays, Triggerfish, and Hailstroms, Oh My: The Fourth Amendment Implications of the Increasing Government Use of Cell-Site Simulators*, 33 TOURO L. REV. 1123, 1126 (2017).

162. Harvey Gee, *Almost Gone: The Vanishing Fourth Amendment's Allowance of Stingray Surveillance in a Post-Carpenter Age*, 28 S. CAL. REV. L. & SOC. JUST. 410, 431 (2019).

163. People v. Gordon, 68 N.Y.S.3d 306, 311 (N.Y. Sup. Ct. 2017); *see* State v. Andrews, 134 A.3d 324 (Md. Ct. Spec. App. 2016).

164. *Andrews*, 134 A.3d at 327.

165. *Id.*

166. *Gordon*, 68 N.Y.S.2d at 311 (describing that a cell site simulator acts as an "instrument of eavesdropping").

167. United States v. Patrick, 842 F.3d 540, 546 (7th Cir. 2016) (Wood, J., dissenting).

168. *Id.* at 543.

169. Ellis v. United States, 270 F. Supp. 3d 1134, 1142 (N.D. Cal. 2017).

C. Cell Tower Dumps

A cellular network is comprised of multiple cell towers, also known as "cell sites."[170] Each network covers three or more directional "sectors."[171] When law enforcement requests information from a cell tower dump, which is a request for CSLI,[172] it receives information from every device that connects to the tower and is also provided the particular time the phone connected to a tower.[173] Requesting information from a tower dump provides access to many individuals' personal data.[174] A tower dump provides information over a short period of time for an unknown number of phones.[175] Tower dumps span broadly instead of deeply.[176]

The use of cell tower dumps has become a "relatively routine investigative technique" by law enforcement officials.[177] Currently, there is no federal statute in effect that addresses how law enforcement officers can request data from a cell tower dump from cell phone providers.[178] The United States Department of Justice encourages assistant United States attorneys to apply for court orders authorizing cell tower dumps in conformance to a provision in the Electronic Communications Privacy Act of 1986.[179]

Not many state and federal courts have addressed cell tower dumps.[180] A Texas court denied the requests for cell tower dumps and held a warrant based on probable cause is required to access the records.[181] On the other

170. Mason Kortz & Christopher Bavitz, *Cell Tower Dumps*, 63 BOSTON BAR J. 26, 26 (2019).

171. *Id.*

172. Michael Price & Bill Wolf, *Building on Carpenter: Six New Fourth Amendment Challenges Every Defense Lawyer Should Consider*, THE CHAMPION, 20, 21 (December 2018), https://www.nacdl.org/getattachment/1616158d-493a-4f1b-a0ba-a2ee5707a87c/price-building-on-carpenter.pdf.

173. John Kelly, *Cellphone Data Spying: It's Not Just the NSA*, USA TODAY (Aug. 11, 2015, 11:51 AM), https://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/.

174. Kortz & Bavitz, *supra* note 170, at 26.

175. Price & Wolf, *supra* note 172, at 21.

176. *Id.* (explaining cell tower dumps can impact hundreds and hundreds of people for a short period, whereas for CSLI tracks one person for a long period of time).

177. Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 2 (2013) (describing in 2013 Verizon received approximately 3,200 warrants or orders for cell tower dumps in 2016, it received approximately 14,630 warrants or orders for cell tower dumps).

178. *Id.*

179. 18 U.S.C. § 3121(a); 99 P.L. 508, 100 Stat. 1848.

180. Owsley, *supra* note 177, at 2.

181. *In re* an Ord. Pursuant to 18 U.S.C. § 2703(d), 964 F. Supp. 2d 674 (S.D. Tex. 2013); *In re* the Search of Cellular Telephone Towers, 945 F. Supp. 2d 769 (S.D. Tex. 2013); *In re* an Ord. Pursuant to 18 U.S.C. § 2703(D), 930 F. Supp. 2d 698 (S.D. Tex. 2012)

hand, a New York court has held that accessing information from cell tower dumps does not constitute a search within the meaning of the Fourth Amendment.[182] A Texas federal district court has noted that a tower dump will presumably affect "hundreds of individuals' privacy interests."[183]

IV. *CARPENTER*'S HOLDING SHOULD BE EXTENDED TO REAL-TIME TRACKING, STINGRAYS, AND CELL TOWER DUMPS

To function in society in the 21st century, nearly everyone has a phone. While the benefit of a phone is that you can call, text, and search for information on your phone, it comes with a threat of privacy invasion via modern technology such as real-time tracking, stingrays, and cell tower dumps. *Carpenter*'s holding should be extended to real-time tracking, stingrays, and cell tower dumps because they are more invasive than CSLI and implicate higher privacy concerns, if not the same, as the majority posed in the *Carpenter* Court. These modern technologies provide an intimate view of a person's life, which can pierce into the lives and homes of people. This information would generally not be available unless a person's reasonable expectation of privacy is invaded.

A. Real-Time Tracking can Provide Precise and Exact Location of a Person and is More Intrusive than CSLI

Even though the *Carpenter* Court did not deal with real-time tracking, its reasoning can be extended to real-time tracking.[184] The multi-factor analysis in *Carpenter* would apply to real-time location data; this kind of data is hidden, continuous, indiscriminate, and intrusive like historical CSLI.[185] In *Carpenter*, Chief Justice Roberts said monitoring a cell phone is akin to using an ankle monitor, which is a "quintessential tracking device."[186] Furthermore, Rule 41 of Federal Rules of Criminal Procedure provides the requirements to obtain a warrant for a tracking device.[187]

(holding cell tower records are protected by the Fourth Amendment and the SCA does not authorize the request for cell tower records).

182. *In re* an Ord. Pursuant to 18 U.S.C. §§ 2703(c) and 2703(d), 42 F. Supp. 3d 511 (S.D.N.Y. 2014).

183. *In re the Search of Cellular Telephone Towers*, 945 F. Supp. 2d at 770 (S.D. Tex. 2013).

184. Sims v. State, 569 S.W.3d 634, 646 (Tex. Crim. App. 2019).

185. Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶ 50 (2007).

186. Freiwald & Smith, *supra* note 14, at 227.

187. FED. R. CRIM. P. 41.

Some courts have held that courts should treat real-time tracking exactly as historical CSLI.[188] Indeed, real-time tracking and historical CSLI should be treated identically because real-time tracking is more intrusive and permeates into an individual's life more than historical CSLI because it can provide the precise and exact location of where a person is currently standing. Like GPS data and historical CSLI, real-time location information is "detailed, encyclopedic, and effortlessly compiled."[189] As with historical CSLI, real-time location information reveals a "detailed chronicle of a person's physical presence compiled . . . every moment."[190] Whether historical CSLI or real-time information is requested, the information provided will be identical; the information that is provided includes the date and time of communications made and received using the phone, telephone numbers involved in these communications, the cell tower the phone was connected to, and call duration.[191]

However, it is also important to consider the *Carpenter* Court's reasoning on why historical CSLI should be considered a more significant intrusion on privacy than the GPS tracking in *Jones*.[192] The *Carpenter* Court suggested historical CSLI is more intrusive than real-time tracking when it stated "[u]nlike with the GPS device in *Jones*, police need not even know in advance whether they want to follow a particular individual, or when."[193] With access to CSLI, the government can now trace a person's approximate historical location, subject to the retention policies of carriers.[194] Carriers currently maintain records of CSLI for up to five years.[195] The government can then access stored data and create a detailed map. In contrast, real-time tracking can only provide information in the moment, and there is not an option to rewind and access data from the past. Though there are strong arguments that historical CSLI is a more significant intrusion than GPS tracking, real-time tracking is much more invasive because it provides "continuous, detailed, and real-time location, speed, direction and duration wherea-

188. Jeremy H. Rothstein, *Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest*, 81 FORDHAM L. REV. 489, 505–06 (2012).

189. Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018).

190. *Id.* at 2220.

191. Christopher Joseph, *Find My Criminals: Fourth Amendment Implications of the Universal Cell Phone App that Every Cell Phone User Has but No Criminal Wants*, 22 BARRY L. REV. 65, 70 (2016).

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

193. *Id.*

194. *Id.*

195. *Id.*

bouts."[196] CSLI tracking is relatively imprecise because it covers a huge geographical area.[197]

Although long-term location information can be comprehensive and disclose intimate details of an individual's daily life, short-term surveillance can be equally as revealing.[198] In *Jones*, Justice Alito, in his concurrence, asserted that constant monitoring of "every single movement" of a person's car for twenty-eight days violated a person's reasonable expectation of privacy and should, for that reason, be deemed a search.[199] He also postulated that short-term tracking would not constitute a search.[200] Justice Alito declined to establish a line that would indicate at what point tracking becomes a search.[201] Justice Sotomayor's concurrence in *Jones* suggested that short-term surveillance could potentially be problematic depending on the amount of information police officers are able to accumulate from aggregate data.[202] Short-term tracking of an individual could reveal private information.[203] For example, attending a religious gathering or political rally can reveal personal information that an individual might want to keep private.[204] Sotomayor was the only Justice who took this position, but did not take an explicit position on whether short-term geolocation monitoring constitutes a search.[205] Nonetheless, it can be inferred from her opinion that Justice Sotomayor believes *any* duration of geolocation surveillance is problematic.[206] While Justice Alito suggests the temporal length of surveillance should be measured, Justice Sotomayor seems more interested in the "*quantity* and *quality*" of information collected.[207] Short-term monitoring generates the same quality of data as long-term monitoring because GPS data "generates a precise, com-

196. Jones, *supra* note 138, at 531 (quoting Lenese C. Herbert, *Challenging the (Un)constitutionality of Governmental GPS Surveillance*, 26 CRIM. JUST. 34, 34 (2011)).

197. *Carpenter*, 138 S. Ct. at 2225.

198. United States v. Jones, 565 U.S. 400, 415–416 (2018) (Sotomayor, J., concurring).

199. *Id.* at 428–31 (Alito, J., concurring).

200. *Id.* at 430.

201. RICHARD M. THOMPSON II, CONG. RESEARCH. SERV., R42511, *UNITED STATES V. JONES:* GPS MONITORING, PROPERTY AND PRIVACY 8 (2012).

202. *Jones*, 565 U.S. at 414 (Sotomayor, J., concurring).

203. Monu Bedi, *Social Networks, Government Surveillance, and the Fourth Amendment Mosaic Theory,* 94 B.U. L. REV. 1809, 1812 (2014).

204. *Id.*

205. *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) ("I agree with Justice Alito that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'" "In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the Katz analysis will require particular attention.").

206. *Id.* at 430.

207. Gabriel R. Schlabach, *Privacy in the Cloud: The Mosaic Theory and the Stored Communications Act*, 67 STAN. L. REV. 677, 684 (2015).

prehensive record of a person's public movements that reflects a wealth of detail about" a person's private life.[208] She further noted

> I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.[209]

Five Justices took the mosaic theory approach.[210] Under the mosaic theory, a search can be analyzed as an aggregation of data rather than individual steps.[211] The notion behind the mosaic theory of the Fourth Amendment is that when it comes to a person's reasonable expectation of privacy, the whole is greater than the sum of its parts.[212] Rather than focusing on individual movements, Justice Sotomayor focused on whether a person has Fourth Amendment rights "in the sum" of his public movements.[213] On the other hand, there is an argument that prolonged surveillance can reveal information that may not be revealed by short-term surveillance, for instance, what a person repeatedly does and does not do.[214]

However, it is important to note the distinction between public movements and private places. *United States v. Knotts* and *United States v. Karo* distinguished the line between public and private space.[215] In *Knotts*, the Court held the warrantless monitoring of a beeper contained in a five-gallon drum of chloroform as it was being transported to a cabin did not implicate the Fourth Amendment because the movements of the vehicle on a public highway were "voluntarily conveyed."[216] Though if law enforcement conducts short-term monitoring of an individual's public movement in a remote

---

208. Peter Toren, *The 'Dirtboxes' of the US Marshalls Service*, HILL BLOG (Dec. 12, 2014, 3:00 PM), https://thehill.com/blogs/congress-blog/judicial/226823-the-dirtboxes-of-the-us-marshals-service.

209. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 GEO. WASH. L. REV. 311, 328 (2012).

210. *Jones*, 565 U.S. at 430 (Alito, J., concurring in the judgment) (embracing the mosaic theory were the following Justices: Sotomayor, Alito, Ginsburg, Breyer, and Kagan).

211. Sohayla M. Roudsari*, Fourth Amendment Jurisprudence in the Age of Big Data: A Fresh Look at the Penumbras Through the Lens of Justice Sotomayor's Concurrence in United States v. Jones*, 9 FED. CTS. L. REV. 139, 156–57 (2016).

212. United States v. Maynard, 615 F.3d 544, 558 (D.C. Cir. 2010) ("[T]he whole of one's movements is not exposed constructively even though each individual movement is exposed, because that whole reveals more—sometimes a great deal more—than the sum of its parts."); *see* Roudsari, *supra* note 211, at 155.

213. Kerr, *supra* note 209, at 328.

214. United States v. Maynard, 615 F.3d 544, 556 (D.C. Cir. 2010).

215. Freiwald & Smith, *supra* note 14, at 207.

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

area where they would not typically be surveilling, it may suggest a reasonable intrusion has occurred.[217] In *Karo*, the Court held that law enforcement monitoring a beeper within a private residence constituted a search within the meaning of the Fourth Amendment.[218] The beeper was hidden in a can of ether.[219] Law enforcement monitoring the beeper obtained information such as if a person was in the home at a specific time.[220] Law enforcement could not have obtained this information by merely observing outside the home.[221]

In the digital world, to exchange ideas or information without revealing information to third parties is impracticable.[222] Compared to 1979, when *Smith v. Maryland* was decided, people disclose more information to third parties now.[223] Justice Sotomayor's concurrence in *Jones* critiqued the third-party doctrine and called it "ill-suited to the digital age."[224] This applies to real-time tracking because individuals convey information about their location while merely carrying their phones.[225] The user of the phone communicates information even when the phone is simply powered on and not being used, so it would be improper to apply the third-party doctrine to real-time tracking—just as it was in *Carpenter*, when the Court chose not to apply the third-party doctrine to historical CSLI.[226]

Furthermore, real-time tracking data should be classified as exhaustive personal data, which is the same as CSLI, instead of limited personal information like pen registers and bank records.[227] Although bank and telephone records may reveal private associations, they do not reveal any information regarding whether a person attended any private meetings or political rallies.[228] In determining whether a reasonable expectation of privacy exists, the length of surveillance should of little importance.[229] Cell phone tracking can quickly and unpredictably invade the right to privacy in a person's home or other private areas because normally phones are carried on one's person.[230] Because a lot of cell phone users keep their cell phone near them or

217. Unite States v. Jones, 565 U.S. 400, 430 (2018) (Alito, J., concurring).
218. United States v. Karo, 468 U.S. 705, 727 (1984) (O'Connor, J., concurring).
219. Freiwald & Smith, *supra* note 14, at 207.
220. *Id.*
221. *Id.*
222. Lindsey Barrett, *Model(ing) Privacy: Empirical Approaches to Privacy Law & Governance*, 35 SANTA CLARA HIGH TECH. L.J. 1, 28 (2018).
223. Rothstein, *supra* note 188, at 508.
224. United States v. Jones, 565 U.S. 400, 415 (2018) (Sotomayor, J., concurring).
225. Jones, *supra* note 138, at 546.
226. *Id.*
227. Carpenter v. United States, 138 S. Ct. 2206, 2219.
228. Jones, *supra* note 138, at 546.
229. *Id.*
230. Tracey v. State, 152 So. 3d 504, 524 (Fla. 2014).

on themselves it is "essentially the corollary of locating the user within the home."[231]

The most common argument is that an individual has no reasonable expectation of privacy in his or her real-time location information because the information is voluntarily conveyed to a third party.[232] However, this argument is weak. It ignores the notion that not all information is conveyed voluntarily.[233] A person voluntarily conveys real-time information when making a call, sending a text or email, but information is not voluntarily conveyed when a user receives calls, texts, messages or emails.[234] While information the user conveyed may be considered "voluntarily" conveyed, that is not the purpose or intention of the user.[235] The information is revealed to use the phone for its intended purpose, not to share location.[236]

In conclusion, real-time tracking is more intrusive than CSLI because it provides detailed and encyclopedic information. Therefore, the Supreme Court should consider it a search within the meaning of the Fourth Amendment. While the *Carpenter* Court argued that CSLI is more invasive than real-time tracking, there are arguments that it's actually the opposite. Real-time tracking is more intrusive and permeates into an individual's life because it can pinpoint the exact location of a person, which CSLI does not. Stingrays, on the other hand, while they do not pinpoint the exact location of a person, are more precise than CSLI because they can locate an individual within a few feet.

B. Stingrays are More Invasive than CSLI, so the Supreme Court Should Extend *Carpenter*'s Holding to Them

The Supreme Court should also extend *Carpenter*'s holding to include stingrays. Protection of stingray data under the Fourth Amendment is compelling because the data is "generated by law enforcement," not the provider, so the third-party doctrine cannot be argued here.[237] Furthermore, sting-

231. *In re* U.S. for an Ord. Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 541 (D. Md. 2011).

232. *See Carpenter*, 138 S. Ct. at 2223–24 (2018) (Kennedy, J., dissenting); *id.* at 2235 (Thomas, J., dissenting); *id.* at 2247 (Alito, J., dissenting); United States v. Riley, 858 F.3d 1012, 1017–18 (6th Cir. 2017); United States v. Davis, 785 F.3d 498, 511–13 (11th Cir. 2015); *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 145–46 (E.D.N.Y. 2013).

233. Jones, *supra* note 138, at 545.

234. *Id.*

235. *Id.*

236. *Id.*

237. Harvey Gee, *Stingray Cell-Site Simulator Surveillance and the Fourth Amendment in the Twenty-First Century: A Review of* The Fourth Amendment in an Age of Surveillance*, and* Unwarranted, 93 ST. JOHN'S L. REV. 325, 342 (2019).

rays function like cell site location tracking because they both use the same technology.[238] Stingrays, however, are more precise than CSLI because they can identify the location of an individual within six feet.[239] They "are invaluable law enforcement tools that locate or identify mobile devices during active criminal investigations,"[240] but, at the same time, implicate significant privacy interests.

Stingrays are much more invasive than CSLI; therefore, if a warrant is required for CSLI, a warrant must be required for the use of cell-site simulators.[241] Because stingrays function unsystematically, in addition to its targeted suspect, "the precise location of every device within [their] range" of innocent people is also obtained.[242] Additionally, the government can at times capture the content of communications when a cell phone is connected to a cell site simulator.[243] This indicates that the government can covertly obtain a vast amount of information.[244] Such a sweeping search effectively functions as a general warrant, which are unconstitutional.[245]

The Framers sought to eliminate general search warrants, which allowed officials to rummage anywhere, even in private homes, to look for contraband.[246] Hence, the government must show probable cause before utilizing a stingray. The government's use of a stingray constitutes a search is because it uses a sense-enhancing device that is not available to the general public to obtain information.[247] The Harris Corporation is the main manufacturer of cell-site simulators and sells them to government agencies.[248] The cell site simulators are listed in a catalogue that is not distributed to the general public or provided in detail on the manufacturer's website; all marketing materials that are circulated contain a warning that if the cell site simulators are sold to anyone other than law enforcement agencies, the person distributing them could potentially be committing a crime and face jail

238. William Curtiss, *Triggering a Closer Review: Direct Acquisition of Cell Site Location Tracking Information and the Argument for Consistency across Statutory Regimes*, 45 COLUM. J.L. & SOC. PROBS. 139, 165 (2011).

239. *Id.*

240. U.S. DEP'T OF HOMELAND SECURITY, POLICY DIRECTIVE 047-02, DEPARTMENT POLICY REGARDING THE USE OF CELL-SITE SIMULATOR TECHNOLOGY 1 (2015), https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf.

241. State v. Sylvestre*,* 254 So. 3d 986, 991 (Fla. Dist. Ct. App. 2018)

242. Browne, *supra* note 159, at 67.

243. Fakhouri & Trimm, *supra* note 152.

244. *Id.*

245. *See id.*

246. Rothstein, *supra* note 188, at 496

247. Cumpstone, *supra* note 8, at 97.

248. Ryan Gallagher, *Meet the Machines that Steal Your Phone's Data*, ARS TECHNICA (Sept 25, 2013, 12:00 PM), https://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/ (last visited Feb. 20, 2021).

time of up to five years.[249] Furthermore, if the targeted individual's cell phone is inside the home, the cell site simulator can follow the cell phone user throughout his or her home and look inside the home, which is similar to what occurred in *Kyllo*, where the government used a thermal-imaging device to look inside Kyllo's home.[250]

In conclusion, stingrays, like real-time tracking, can provide more precise location information compared to CSLI. Stingrays are also akin to a *Kyllo* search. Thus, stingrays are more invasive than CSLI. Since the Supreme Court considered CSLI a search within the meaning of the Fourth Amendment, it should consider stingrays a search within the meaning of Fourth Amendment. Cell tower dumps, on the other hand, while they provide less information, provide information of the privacies of an individual's life.

C. Cell Tower Dumps are the Equivalent of Dragnet Surveillance, so They Should Be Treated Like CSLI

Lower courts are currently divided on how cell tower dumps should be treated under the Fourth Amendment.[251] Though the Supreme Court has yet to address cell tower dumps, it has suggested that "dragnet surveillance" is unlawful. The *Carpenter* Court suggested that real-time tracking and the use of stingrays could be considered dragnet surveillance, and since cell tower dumps are analogous in nature to both real-time tracking and the use of

249. *Id.*

250. Kyllo v. United States, 533 U.S. 27, 29–30 (2001).

251. RACHEL LEVINSON-WALDMAN, CELLPHONES, LAW ENFORCEMENT, AND THE RIGHT TO PRIVACY 3 (2018); *see In re* Cell Tower Records Under 18 U.S.C. 2703(D), 90 F. Supp. 3d 673, 675 (S.D. Tex. 2015) (holding that a court order was sufficient, and stating that "cell tower logs requested here [are] categorized as ordinary business records entitled to no constitutional protection"); *In re* an Ord. Pursuant to 18 U.S.C. 2703(c), 42 F Supp. 3d 511, 519 (S.D.N.Y. 2014) (finding a court order sufficed because § 2703(d) of the Stored Communications Act applied to cell tower dumps and the third-party doctrine destroyed protections under the Fourth Amendment, but requiring "an amended application that (1) provides more specific justification for the time period for which the records will be gathered and (2) outlines a protocol to address how the Government will handle the private information of innocent third-parties whose data is retrieved"); *see also* Hewitt v. United States, No. 3:08-CR167-B (2), 2018 WL 3853708, at *5 (N.D. Tex. July 25, 2018), report and recommendation adopted, 3:08-CR-167-B (2), 2018 WL 3845232 (N.D. Tex. Aug. 13, 2018) (holding that "[t]he Fourth Amendment does not prohibit the government from obtaining historical cell tower data for all cell phones used at the time of a crime"); United States v. Pembrook, 119 F. Supp. 3d 577, 585 (E.D. Mich. 2015) (holding because the government's lack of a warrant was not deliberate or grossly negligent, the data of the cell tower dump need not be suppressed); United States v. Scott, No. 14-20780, 2015 WL 4644963, at *7 (E.D. Mich. 2015) (holding that when the cell phones are within the tower's range, the individual has no reasonable expectation of privacy in records).

stingrays, cell tower dumps should fall under this category.[252] Though the data is short term tracking, law enforcement also requests from mobile carriers detailed information such as GPS location data, website addresses, and, in some cases, search terms entered into cell phones.[253] Cell tower dumps are only limited in their geographic scope.[254]

Carpenter emphasizes that an individual has a reasonable expectation of privacy in his or her historical cellphone location data.[255] *Carpenter*'s holding should extend to cell tower dumps because information acquired through them can expose the "privacies of life."[256] The government's use of cell-tower dumps violates an individual's reasonable expectation of privacy.[257] Cell tower dumps are known as "virtual time machine[s]."[258] A cell tower dump can provide an intimate window into the privacies of life such as familial, political, and religious associations.[259] Cell tower dumps reveal less information over time compared to CSLI; however, they do involve access to more users' data compared to historical CSLI.[260] Furthermore, at least one United States Magistrate Judge has suggested that the Fourth Amendment impliedly protects information gathered in cell tower dumps.[261]

Although cell tower dumps involve the privacy of many individuals, they can be considered less intrusive on an individual level.[262] Cell tower dumps cover a short period of time and a small area.[263] Law enforcement is not seeking information about a specific user or cell phone number.[264] It looks at cell phones within a certain geographical area on a given date and time.[265] Cell tower data provides general location of the cell phone.[266] Fur-

252. Kortz & Bavitz, *supra* note 170, at 27.

253. Ellen Nakashima, *Agencies Collected Data on Americans' Cellphone Use in Thousands of 'Tower Dumps'*, WASH. POST (Dec. 9, 2013), https://www.washingtonpost.com/world/national-security/agencies-collected-data-on-americans-cellphone-use-in-thousands-of-tower-dumps/2013/12/08/20549190-5e80-11e3-be07-006c776266ed_story.html.

254. Nate Anderson, *How "Cell Tower Dumps" Caught the High Country Bandits—and Why It Matters*, ARS TECHNICA (Aug, 29, 2013), https://arstechnica.com/tech-policy/2013/08/how-cell-tower-dumps-caught-the-high-country-bandits-and-why-it-matters/.

255. Carpenter v. United States*,* 138 S. Ct. 2206, 2219 (2018); *see also* Price & Wolf, *supra* note 172, at 21.

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

257. Price & Wolf, *supra* note 172, at 21.

258*. Id.*

259*. Id.*

260*. Id.* at 26.

261. *In re* an Ord. Pursuant to 18 U.S.C. 2703(d) Directing Providers to Provide Historic Cell Site Locations Records, 930 F. Supp. 2d 698, 700 (S.D. Tex. 2012).

262. Kortz & Bavitz, *supra* note 170, at 27.

263*. Id.*

264. Amanda Regan, Note, *Dumping the Probable Cause Requirement: Why the Supreme Court Should Decide Probable Cause Is Not Necessary for Cell Tower Dumps*, 43 HOFSTRA L. REV. 1189, 1220 (2015).

265*. Id.*

thermore, cell tower data is less precise compared to GPS technology.[267] The precision depends on the range of the geographical area covered by the cell site.[268] The greater the clustering of cell sites, the smaller the coverage area.[269] In an urban area, cell site records can be imprecise up to forty times because it can cover hundreds of city blocks.[270] Thus, in *United States v. Adkinson*, *Carpenter*'s holding was not extended to tower dumps in part because the *Carpenter* Court had declined to rule that cell tower dumps were searches requiring warrants.[271]

However, while historical CSLI data received from cell tower dumps for less than seven days is not as intrusive as the longer-term data *Carpenter* addressed, because cell tower data is a subset of historical CSLI[272], it should be considered a search within the meaning of the Fourth Amendment. Cell tower dumps are a "limited dragnet."[273] When a law enforcement officer requests a cell tower dump, he or she is requesting information "on all calls transmitted through a cell tower at a given time, on a given date, near a specific location."[274] Because the officer is not aware of the suspect's phone number, the officer must go through all cell service provider records and find all cell phones that were near the cell tower for the date and time that he is looking for records.[275] Thus, because a cell tower dump collects enormous amount of data, it constitutes as dragnet surveillance, which the Supreme Court has held is unconstitutional.[276]

In conclusion, the Supreme Court should consider cell tower dumps a search within the meaning of the Fourth Amendment. While cell tower dumps do not provide as much information as real-time tracking or stingrays, they reveal the privacies of an individual's life such as familial and political information. The use of cell tower dumps violates an individual's reasonable expectation of privacy as the data involves information for many individuals. To prevent the invasion of privacy, Congress can enact exhaustion laws.

266. Owsley, *supra* note 177, at 6.
267. Regan*, supra* note 264, at 1208.
268. *Carpenter*, 138 S. Ct. at 2211.
269. *Id.*
270. *Id.* at 2225. (Kennedy, J., dissenting).
271. United States v. Adkinson, 916 F.3d 605, 611 (11th Cir. 2019).
272. Regan, *supra* note 264, at 1190.
273. *Id.*
274. *Id.*
275. *Id.* at 1191.
276. Kortz & Bavitz, *supra* note 170, at 26.

V. RECOMMENDATIONS

Because modern technology has advanced to the point where the exact location of an individual can be determined, Congress must enact electronic "exhaustion" requirements for surveillance to protect individual from an invasion of privacy. This would ensure that intrusive surveillance only occurs when it is absolutely necessary.

A. Recommendations for Congress to Prevent Invasion of Privacy

The Supreme Court has acknowledged that this is the "Cyber Age."[277] Before the digital era, Congress passed the Stored Communications Act (SCA) in 1986.[278] The SCA furnishes a scheme to determine when the government can obtain certain kinds of electronically stored information (ESI) from third-party providers.[279] It also sets forth the various tools government officials can use to access ESI, such as obtaining warrants or court orders and permitting searches without a notice.[280] When the government provides "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication are relevant and material" to an investigation underway, then the government can request records.[281]

Because location data is sensitive, obtaining location information should require not only a warrant, but also exhaustion.[282] The Wiretap Act has an exhaustion requirement and is a good model to follow.[283] The Wiretap Act states that less invasive investigative procedures must be attempted first.[284] In order for the government to show that it has met the exhaustion requirement, it must provide more than a standard recitation of the difficulties it faced in gathering usable evidence.[285] "[T]he adequacy of [the government's] showing is to be tested in a practical and commonsense fashion

---

277. *Carpenter*, 138 S. Ct. at 2224 (Kennedy, J., dissenting) ("It is true that the Cyber Age has vast potential both to expand and restrict individual freedoms in dimensions not contemplated in earlier times.")

278. 18 U.S.C. § 2703.

279. *Id.*

280. *Id.*

281. § 2703(d) (explaining that contents are permitted only in limited circumstances).

282. 18 U.S.C § 2518(1)(c) ("[A] full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous.").

283. *Id.* (The Wiretap Act governs warrants for intercepting communications).

284. Jake Laperruque, *Congress Should Place More Limits on Cellphone Location Tracking After Carpenter,* JUST SECURITY, https://www.justsecurity.org/54231/probable-cause-electronic-exhaustion-limits-location-tracking-carpenter/ (last visited Dec. 18, 2019).

285. United States v. Oriakhi, 57 F.3d 1290, 1297 (1995).

that does not hamper unduly the investigative powers of law enforcement agents."[286] Including an exhaustion requirement would ensure that an intrusive form of surveillance occurs only when it is necessary.[287] When the court is dealing with cellphone tracking, *electronic* investigative procedures should be required to be exhausted before more intrusive approaches are utilized.[288] Electronic exhaustion would prevent an invasion of privacy.

Limiting governmental use of geolocation information for surveillance prevents abusive access and utilization of private individuals' geolocation information. The Geolocation Privacy and Surveillance (GPS) Act has been proposed a few times but has not progressed in the House and Senate Judiciary committees.[289] The GPS Act is a bill that was introduced in order to combat the encroachment on an individual's privacy during the cyber age.[290] The Act lists procedures to which law enforcement must adhere in order to "track an individual's whereabouts"; in addition, it prohibits the disclosure or dissemination of an individual's geolocation information or data without the individual's consent.[291] The GPS Act would protect real-time tracking and "access to records of individuals' past movements."[292]

In conclusion, enacting exhaustion laws and the passage of the GPS bill will provide protection to an individual's location and access of those records. In the long run, these measures will protect activities protected under the First Amendment. If there are no exhaustion laws in place, if the government obtains a warrant, it would be able to place cell tower dumps, stingrays, and use real-time tracking information at political rallies and protests. This would not only target one person, but everyone involved in these settings. Thus, the warrant would create a pretext to install these modern technological devices. If invasive surveillance is necessary, it should only be limited to the particular individual or the smallest geographic area.

VI. CONCLUSION

In 1791, when the states ratified the Fourth Amendment, the Framers had no perception of the technological advances that would one day become an issue under the Fourth Amendment. These advances have made possible

286. *Id.* (quoting United States v. Smith, 31 F.3d 1294, 1297 (4th Cir. 1994)).
287. *Id.*
288. *Id.*
289. *Geolocation Privacy Legislation*, GPS.GOV, https://www.gps.gov/policy/legislation/gps-act/ (last visited Oct. 22, 2019).
290. Katherine A. Mitchell, *The Privacy Hierarchy: A Comparative Analysis of the Intimate Privacy Protection Act vs. the Geolocational Privacy and Surveillance Act*, 73 U. MIAMI L. REV. 569, 571 (2019).
291. *Id.*
292. *GPS Act*, RON WIDEN, UNITED STATES SENATOR FOR OREGON, https://www.wyden.senate.gov/priorities/gps-act (last visited Oct. 22, 2019).

ever-increasing intrusions into the privacies of life. Even when an individual is not using his or her phone, the phone is transmitting data. The world has come a long way— from sending a telegram, to making a call, to using the internet, to gadgets that can track and pinpoint a user's exact location. Because the Supreme Court has decided that historical CSLI requires a warrant, it should extend that reasoning to newer, parallel technology like real-time tracking, stingrays, and cell tower dumps—all more invasive than historical CSLI.

People do not buy phones to share their information with government officials or the police. They buy them to talk to their loved ones and friends and connect with other people. Hence, they buy them to function in modern society. The use of real-time tracking, stingrays, and cell tower dumps is an infringement of an individual's reasonable expectation of privacy. Any police activity that is the "modern-day equivalent of activity" that has been restricted in the past should also be restricted today.[293] Within the last twenty years, technological advancements have turned cell phones into mini-computers that people can carry in their pockets, making it easy for the government to invade individuals' privacy.

The eruption of modern technology has increased law enforcement's ability to thoroughly investigate crimes and efficiently respond to situations. In an effort to make arrests or provide protection to citizens of the community, law enforcement has exceeded its power to obtain personal information that would otherwise not be known. In order to balance the interests and harms of society, it is also important to impose limitations upon law enforcement to prevent abuse or overly pervasive surveillance. The enactment of exhaustion requirements will prevent the encroachment of an individual's reasonable expectation of privacy. The government must use less invasive investigative procedures first before it requests location records of an individual. As technology involves, it is important that Congress takes important measures to protect the interests of individuals.

*Deepali Lal**

293. Ohm, *supra* note 102, at 394.

* J.D. Candidate at the University of Arkansas at Little Rock William H. Bowen School of Law, expected graduation May 2021. B.B.A. in International Business and Human Resource Management, University of Arkansas at Little Rock. I want to thank my parents and my sisters for their support and encouragement. I also want to express my immense gratitude to Professor Nicholas Kahn-Fogel for mentoring and investing in me throughout the entire process. Finally, I would like to thank the UALR Law Review staff for their remarkable support and guidance.