THE FOURTH AMENDMENT COVERS "FOG REVEAL": NOT THE OTHER WAY AROUND

CONNOR REID†

I. INTRODUCTION

Davin Hall began working with the Greensboro Police Department ("GPD") as a crime analyst in 2014.[1] Through his analysis, Hall helped police patrol identify patterns in criminal offenses around the city.[2] During his six years with the GPD, Hall frequently relied on software applications to make his work with crime data more efficient and user-friendly.[3] Initially, Hall thought nothing of it when the GPD announced its plan to implement a software application called "Fog Reveal" as part of its crime surveillance efforts.[4] Shortly after the GPD began using Fog Reveal, Hall began to develop concerns about the privacy threats the software posed to the citizens of Greensboro.[5] Fog Reveal allowed the GPD to search through the digital information stored on every mobile device within a selected location and timeframe.[6] According to Hall, "Anyone who is in the area that's being captured can have their devices picked up by [Fog Reveal] and any device can be searched without a warrant . . . ."[7] With access to a device's digital information, law enforcement can determine where the owner of a captured mobile device lives, where they work, and with whom they associate.[8] After Hall's concerns

† J.D. Candidate 2024, Wake Forest University School of Law; Political Science, B.S. 2021, Appalachian State University. I want to express my sincere gratitude to Professor Alyse Bertenthal, whose commitment to fostering a deep understanding of the intricacies of criminal law has undoubtedly been instrumental in shaping the ideas presented in this article. I am also profoundly thankful for the mentorship of Missy Owen, whose wisdom and encouragement have been a constant source of inspiration.

1. Sayaka Matsuoka, *Public Records Request Shows Greensboro Police Department Used Mobile Tracking Surveillance Tech*, TRIAD CITY BEAT (Dec. 1, 2022), https://triad-city-beat.com/public-records-request-shows-greensboro-police-department-used-mobile-tracking-surveillance-tech.
2. *Id.*
3. *Id.*
4. *Id.*
5. *Id.*
6. *Id.*
7. *Id.*
8. *Id.*

were dismissed by police, attorneys, and the Greensboro City Council, he resigned from the GPD in late 2020.[9] The City of Greensboro defended the GPD's use of Fog Reveal, claiming that because the mobile identification numbers Fog Reveal captures do not "contain any personally identifiable information, it was fair game as a search."[10] However, as Hall pointed out, if Fog Reveal did not provide access to personal information, law enforcement agencies "wouldn't want it."[11] As of 2022, nearly two dozen government agencies had contracts with Fog Reveal.[12]

Law enforcement's use of software applications, like Fog Reveal, is emblematic of the growing number of areas where digital data is utilized in today's rapidly advancing technological landscape. The increasing ubiquity of smartphones has placed an unprecedented economic premium on personal data. Indeed, personal information is an essential currency in the new millennium.[13] Some scholars describe this trend as "the commodification of our digital identity."[14] Recently, companies have discovered ways to use the personal data stored on smartphones for commercial purposes.[15] For example, companies use personal data to analyze consumer behavior through prediction analytics and data profiling to generate revenue.[16] These technological trends have significant implications on the expectation of privacy American citizens have over personal information stored on their mobile devices.

Whatever one's feelings about the privacy risks surrounding the commercial use of personal data, graver privacy concerns are implicated when law enforcement agencies use personal data to deprive an individual of their liberty. Part II of this Note discusses the Fourth Amendment and how government agencies use the "Data Broker Loophole" to avoid obtaining a search warrant before purchasing cell phone location information. Part III contends that current Supreme Court precedent prohibits the government's purchase of digital location information and its subsequent use in criminal investigations, focusing on constitutional and public policy arguments. Finally, Part IV proposes solutions available to the judiciary and legislature to strengthen the privacy expectations that American citizens have over their cell phone location data.

---

9. *Id.*

10. *Id.*

11. *Id.*

12. Garance Burke & Jason Dearen, *Tech Tool Offers Police 'Mass Surveillance on a Budget'*, AP NEWS (Sept. 2, 2022, 5:28 PM), https://apnews.com/article/technology-police-government-surveillance-d395409ef5a8c6c3f6cdab5b1d0e27ef.

13. Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056, 2056 (2004).

14. Milena Mursia & Carmine A. Trovato, *The Commodification of Our Digital Identity*, FILODIRITTO (May 31, 2021), https://www.filodiritto.com/commodification-our-digital-identity.

15. *Id.*

16. Blaire Rose, *The Commodification of Personal Data and the Road to Consumer Autonomy Through the CCPA*, 15 BROOK. J. CORP. FIN. & COM. L. 521, 527 (2021).

II. BACKGROUND

A. The Fourth Amendment and The Reasonable Expectation of Privacy

The Fourth Amendment recognizes in relevant part "[t]he 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 . . . ."[17] The ratification of the Fourth Amendment was the Founders' response to the "general warrants" and "writs of assistance," which allowed British officers to rummage through homes unimpeded to search for evidence of criminal activity.[18] In 1791, the government had to physically intrude into the home to acquire personal information about an individual. Due to the technological advancements made throughout the twentieth and twenty-first centuries, law enforcement now possesses a dizzying array of sophisticated surveillance technologies to collect information about an individual without setting foot on their property or making contact with them in person.[19] As a result, the Supreme Court's Fourth Amendment jurisprudence has evolved alongside technological advancements to ensure that Fourth Amendment protections remain as robust as they were in 1791. As stated by the late Supreme Court Justice Scalia, "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[20] With these principles in mind, it is imperative that the Supreme Court's Fourth Amendment jurisprudence keeps pace with technological advancement, lest American citizens only be free from antiquated forms of government intrusion.

Generally, government agencies seeking access to Americans' personal electronic data must comply with a legal process to obtain that data.[21] "That process can be mandated by the Constitution (the Fourth Amendment's warrant and probable cause requirement) or by statute (such as the federal Electronic Communications Privacy Act, or various state laws)."[22] Ostensibly, the government's purchase of digital data that reveals an individual's physical movements is restricted by the above sources. However, as it turns out,

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

18. Riley v. California, 573 U.S. 373, 403 (2014).

19. *See generally* Emily A. Vogels et al., *Tech Causes More Problems than It Solves*, PEW RSCH. CTR. (June 30, 2020), https://www.pewresearch.org/internet/2020/06/30/tech-causes-more-problems-than-it-solves.

20. Kyllo v. United States, 533 U.S. 27, 33–34 (2001).

21. Sharon Bradford Franklin et al., *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers*, CTR. FOR DEMOCRACY & TECH. (Dec. 9, 2021), https://cdt.org/insights/report-legal-loopholes-and-data-for-dollars-how-law-enforcement-and-intelligence-agencies-are-buying-your-data-from-brokers.

22. *Id.*

government agencies currently avoid judicial and legislative oversight by purchasing digital information from third-party data brokers.[23]

B. Supreme Court Precedent on Cellular Data

The Fourth Amendment is the most vital source of individual privacy protection against governmental intrusion. In *Katz v. United States*, the Supreme Court held that the government must obtain a warrant based on probable cause before intruding upon a person's house, papers, and effects where that person (1) exhibits an actual expectation of privacy that (2) society recognizes as reasonable.[24] The relevant question is then: over what matters do American citizens have a reasonable expectation of privacy triggering the Fourth Amendment's safeguards? More specifically, for this Note, what level of privacy protection should be afforded to digital data stored on cell phones?

Although no clear test exists to determine which expectations of privacy are entitled to protection, the Supreme Court uses two guideposts to aid in their analysis.[25] First, the Fourth Amendment "seeks to secure 'the privacies of life' against 'arbitrary power,'" and second, "a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'"[26] In *Carpenter v. United States*, the Supreme Court was asked to determine whether an individual has a reasonable expectation of privacy over the cell-site location information ("CSLI") that is generated when an individual's phone connects to a cell tower.[27] CSLI provides a cell phone's approximate location.[28] In that case, Carpenter (the "Petitioner") was charged with six counts of robbery.[29]

At trial, an FBI agent offered expert testimony about Petitioner's CSLI which placed him near four of the robberies he was charged with.[30] Petitioner was convicted on all of the robbery charges and was sentenced to more than one hundred years in prison.[31] On appeal, Petitioner argued that the FBI's use of the CSLI constituted a search and thus the FBI needed a warrant before obtaining the CSLI.[32] The Supreme Court agreed, holding that when the FBI accessed Petitioner's CSLI, it conducted a search within the meaning

23. *See id.*

24. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J. concurring).

25. Carpenter v. United States, 138 S. Ct. 2206, 2213–14 (2018).

26. *Carpenter*, 138 S. Ct. at 2214 (first quoting Boyd v. United States, 116 U.S. 616, 630 (1886); and then quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

27. *See Carpenter*, 138 S. Ct. at 2211–12.

28. *Cell Phone Location Tracking*, NAT'L ASS'N OF CRIM. DEF. L. (Apr. 17, 2019), https://www.nacdl.org/Document/2016-06-07_CellTrackingPrimer_Final(v2)(2).

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

30. *Id.* at 2212–13.

31. *Id.* at 2213.

32. *Id.* at 2212.

of the Fourth Amendment triggering the warrant requirement.[33] In reaching its holding, the Court recognized that individuals maintain a reasonable "expectation of privacy in the record of [their] physical movements as captured through CSLI."[34] Moreover, the Court declined to apply the third-party doctrine, which states that individuals do not have a reasonable "expectation of privacy in information [they] voluntarily turn[ed] over to third parties."[35] The Court reasoned that the third-party doctrine established in *Miller* was inapplicable to CSLI because an individual maintains a reasonable expectation of privacy in the record of their physical movements, even if the government leverages the technology of a third party to obtain that information.[36]

A reasonable interpretation of the Supreme Court's holding in *Carpenter* is that law enforcement must obtain a search warrant before obtaining the location information that is created when a person uses their cell phone. However, law enforcement agencies nationwide are currently using surveillance tools that reveal more accurate and detailed location information than is revealed by CSLI without obtaining a warrant.[37]

C. The Electronic Communications Privacy Act

Another potential source of privacy protection over cellular data is the Electronic Communications Privacy Act ("ECPA").[38] Congress passed the ECPA to restrict the government's ability to access digital information without following specified legal standards.[39] In doing so, the ECPA defines categories of electronic service providers whose customer information is subject to heightened protections.[40] The Act recognizes two types of service providers: (1) a Remote Computing Service ("RCS"), and (2) an Electronic Communication Service ("ECS"). An RCS is any service that gives the public "computer storage or processing services by means of an electronic communications system."[41] An electronic bulletin board is an example of a "remote computing service" under 18 U.S.C. § 2711(2).[42] An ECS is "any service which provides to users thereof the ability to send or receive

33. *Id.* at 2217.
34. *Id.*
35. *Id.* at 2216–17 (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).
36. *Id.* at 2217.
37. Burke & Dearen, *supra* note 12.
38. *See generally* 18 U.S.C. §§ 2510–23.
39. *See* Franklin et al., *supra* note 21 (listing legal protections regulating access to personal data by government agencies).
40. *See* 18 U.S.C. § 2711(2) (defining the "remote computing service" category); 18 U.S.C. § 2510(15) (defining the "electronic communication service" category).
41. 18 U.S.C. § 2711(2).
42. Steve Jackson Games, Inc. v. United States Secret Serv., 816 F. Supp. 432, 443 (W.D. Tex. 1993).

wire or electronic communications."[43] Telephone and electronic mail companies are ECS providers.[44] ECS providers cannot disclose to third parties "the contents of a communication while in electronic store by that service," while an RCS provider cannot disclose the "contents of any communication which is carried or maintained on that service."[45] RCS and ECS providers are prohibited from "knowingly divulg[ing] a record or other information pertaining to a subscriber to or customer of such service . . . to any governmental entity."[46] This also prohibits these providers from selling such information to the government.[47]

The ECPA establishes a specific legal process the government must follow to access customer information from either an RCS or ECS.[48] To obtain non-content information—which includes transactional data such as the duration or size of the communication—the government must demonstrate reasonable suspicion of "'specific and articulable facts showing that there are reasonable grounds to believe' that the information [sought] is 'relevant and material to an ongoing criminal investigation.'"[49] The reasonable suspicion requirement is less stringent than the probable cause requirement.[50] Where the government wishes to access the content of an electronic communication, it must obtain a warrant supported by probable cause.[51] Despite Congress's intent to promote "the privacy expectation of citizens" in passing the ECPA, government agencies have learned to avoid the ECPA's restrictions by carefully selecting from whom the information is purchased.[52]

D. Fog Reveal

Fog Reveal is a pay-for-access web tool that enables government agencies in the U.S. to engage in warrantless surveillance of individuals, groups, and places.[53] The tool was developed by Fog Data Science ("FDS"), a limited liability company founded in 2016 by two former Department of Homeland Security

43. 18 U.S.C. § 2510(15).

44. *See* S. REP. NO. 99-541, at 2–3 (1986) (discussing the operation of telephone and electronic mail).

45. 18 U.S.C. §§ 2702(a)(1)–(a)(2).

46. 18 U.S.C. § 2702(a)(3).

47. Franklin et al., *supra* note 21.

48. *See id.*

49. *Id.* (quoting Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018)).

50. Franklin et al., *supra* note 21.

51. United States v. Warshak, 631 F.3d 266, 274, 285 (6th Cir. 2010).

52. H.R. REP. NO. 99-647, at 19 (1986).

53. Anne Toomey McKenna, *What is Fog Reveal? Legal Scholar Explains App Some Police Forces Are Using to Track People Without Warrant*, STUDY FINDS (Oct. 19, 2022), https://studyfinds.org/what-is-fog-reveal.

officials under former President George W. Bush.[54] FDS currently possesses billions of data points from over 250 million U.S. mobile devices.[55] The way Fog Reveal works is simple: FDS purchases location data from smartphone applications that target ads based on a person's movements and interests, and then offers that data to law enforcement agencies for a subscription fee.[56] Once the subscription fee is paid, the subscriber gains access to Fog Reveal.[57] Law enforcement agencies that have Fog Reveal subscriptions gain access to the identification of every mobile device within the geographical area and timeframe specified by law enforcement.[58] The location data provides "pattern of life analysis," which reveals where a device owner "sleeps, studies, works, worships, and otherwise associates."[59] Although FDS claims that it never collects personally identifiable information, pattern of life analysis allows law enforcement to learn the identity of device owners.[60]

The location data provided by FDS and Fog Reveal reveals where a person sleeps at night, which in turn discloses where that person lives.[61] From there, it is easy to imagine how Fog Reveal might reveal one's personal identity.[62] A study conducted nearly a decade ago found that just four spatial-temporal data points were sufficient to identify ninety-five percent of the one and a half million people in the data set.[63] A Missouri official who worked closely with Fog Reveal confirmed these suspicions in 2019 when he wrote that although Fog Reveal's data does not technically reveal personal information, "if we are good at what we do, we should be able to figure out the owner."[64]

According to GovSpend, a company that tracks government spending, as of September 2022, nearly two dozen government agencies subscribed to Fog Reveal.[65] The data accessed through Fog Reveal implicates grave privacy concerns for every American citizen who uses a smartphone. Moreover, law enforcement's use of personal data in connection with criminal investigations raises serious questions about the reach of Fourth Amendment privacy protections and the sufficiency of current Supreme Court precedent and federal privacy laws.

---

54. Burke & Dearen, *supra* note 12.

55. McKenna, *supra* note 53.

56. *Id.*

57. *Id.*

58. Marc Dahan, *What is Fog Data Science and Why Should You Care?*, COMPARITECH (Jan. 2, 2023), https://www.comparitech.com/blog/information-security/fog-data-science.

59. *Id.*

60. *Id.*

61. *Id.*

62. *Id.*

63. Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, 3:1376 SCI. REP., Mar. 2013, at 3.

64. *Thanks to Tech, Police Practice "Mass Surveillance on a Budget" – No Warrant Required*, CBS NEWS (Sep. 1, 2022, 5:34 PM), https://www.cbsnews.com/news/police-mass-surveillance-fog-reveal-tech-tool.

65. Burke & Dearen, *supra* note 12.

E. The Data Broker Loophole

Given the Supreme Court's recognition of an individual's reasonable expectation of privacy in the record of their physical movements, one would assume that a formidable constitutional hurdle confronts law enforcement agencies seeking to use surveillance tools that reveal more than simply a person's physical movements. However, the privacy protections guaranteed by the Fourth Amendment have yet to invalidate law enforcement agencies' use of software applications like Fog Reveal.[66] The critical distinction seemingly placing Fog Reveal beyond the reach of the Supreme Court's holding in *Carpenter* is the fact that when law enforcement agencies use Fog Reveal, they are purchasing data from a private third-party broker.[67] In contrast, the FBI in *Carpenter* obtained the Petitioner's CSLI through a compulsory legal process.[68] This arbitrary distinction that allows law enforcement to evade the requirements of the Fourth Amendment by purchasing data from third-party brokers has been described as the "Data Broker Loophole."[69] According to Kentucky Senator Rand Paul, the "Data Broker Loophole" allows the government to buy "its way around the Bill of Rights by purchasing the personal and location data of everyday Americans."[70] The view of the Defense Intelligence Agency ("DIA"), which admits to purchasing commercial location data, is that the Supreme Court's decision in *Carpenter* only applies to location data obtained through a compulsory legal process and not data purchased by the government.[71]

Law enforcement agencies also use the "Data Broker Loophole" to get around the ECPA requirements. The ECPA allows RCS and ECS providers to voluntarily provide non-content information to non-government third parties that are not RCS or ECS providers.[72] This loophole enables ECS and RCS providers to voluntarily sell data to private third parties like Fog Data Sciences, which are then able to sell the data to government agencies.[73] As a result, all a government

66. *See, e.g.*, *Carpenter*, 138 S. Ct at 2217.

67. McKenna, *supra* note 53.

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

69. *Bipartisan Coalition Responds to the FBI's New Policies Under Foreign Intelligence Surveillance Authority*, BRENNAN CTR. FOR JUST. (June 13, 2023), https://www.brennan center.org/our-work/analysis-opinion/bipartisan-coalition-responds-fbis-new-policies-under-foreign.

70. *Wyden, Paul and Bipartisan Members of Congress Introduce The Fourth Amendment Is Not For Sale Act*, RON WYDEN U.S. SENATOR FOR OR. (Apr. 21, 2021), https://www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-members-of-congress-introduce-the-fourth-amendment-is-not-for-sale-act-.

71. William S. Stewart, *Clarification of Information Briefed During DIA's 1 December Briefing on CTD,* DEF. INTEL. AGENCY 1, 1–2 (Jan. 15, 2021), https://int.nyt.com/data/documenttools/dia-memo-for-wyden-on-commercially-available-smartphone-locational-data/d7d41dccdd1d46b0/full.pdf.

72. Franklin et al., *supra* note 21.

73. *See id.*

agency has to do to obtain information from RCS and ECS providers without a warrant is use a middleman like Fog Data Sciences to purchase the data first.[74]

The Supreme Court's holding in *Carpenter* and Congress's purpose in passing the ECPA reflect a fervent commitment to restricting the government's access to Americans' digital information. That government agencies across the United States can use Fog Reveal without judicial or legislative oversight flies in the face of the reasonable expectations of privacy already recognized by the Supreme Court.

III. THE DATA BROKER LOOPHOLE: A CHEAP READING OF *CARPENTER*

This section offers constitutional and social policy reasons supporting *Carpenter's* applicability to the government's use of Fog Reveal. This section also discusses solutions available to the judiciary and legislature to enhance privacy protections over digital information.

A. Carpenter and the Fourth Amendment's Warrant Requirement Apply to The Government's Use of Fog Reveal

The arguments made by Fog Data Sciences and the government agencies it contracts with in support of *Carpenter's* inapplicability to Fog Reveal are inconsistent with the *Carpenter* holding and the considerations that have long guided the Supreme Court's Fourth Amendment jurisprudence. As technological enhancements expand the government's capacity to intrude into areas normally guarded against curious eyes, the Supreme Court has sought to "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[75] Interpreting *Carpenter* to not apply to law enforcement's use of Fog Reveal is antithetical to the Supreme Court's commitment to preserving privacy protections under the Fourth Amendment.[76]

B. The Fourth Amendment Protects People and Not Simply Areas

Central to modern Fourth Amendment jurisprudence is the understanding that the "Fourth Amendment protects people—and not simply 'areas'—[from] unreasonable searches and seizures."[77] As

74. *Id.*
75. *Kyllo*, 533 U.S. at 34.
76. Franklin et al., *supra* note 21.
77. *Katz*, 389 U.S. at 353.

explained in *Katz*, the emphasis on people rather than areas prevents arbitrary interpretation from eroding the safeguards of the Fourth Amendment. For example, a person who knowingly exposes information to the public has no reasonable expectation of privacy over that information under the Fourth Amendment even if the disclosure took place from the privacy of the individual's home.[78] On the other hand, a person who seeks to keep information private may be entitled to Fourth Amendment protections even when they are in a public area.[79] In other words, a person who makes a private phone call in public is entitled to the same Fourth Amendment privacy protections as someone who makes a private phone call from their bedroom. The Fourth Amendment analysis in this situation turns on whether a person has a reasonable expectation of privacy over their private telephone calls, not where they are located when making those private telephone calls.

Government agencies in favor of using applications like Fog Reveal cling to the Fourth Amendment analysis the Supreme Court rejected in *Katz*. Proponents of Fog Reveal concede that Americans have a reasonable expectation of privacy over digital data that records their physical movements.[80] However, they contend that under *Carpenter*, Americans do not have a reasonable expectation of privacy over that digital data when purchased from a third-party broker.[81] The arbitrary distinction drawn from data obtained through a compulsory legal process and that obtained from a third-party broker is analogous to the arbitrary distinction in *Katz* between telephone booth and home.[82] The Court in *Katz* focused its Fourth Amendment analysis not on *where* the telephone call occurred, but on the privacy expectations of the *person* who made the call.[83] With respect to Fog Reveal, the Fourth Amendment analysis does not turn on *where* the digital information is located when the government obtains it, but on the privacy expectations of the *person* whose information is revealed.[84] To hold otherwise would base privacy protections over digital information on the area the data is located, rather than the person who is affected. Because the Fourth Amendment protects people—and not simply areas—*Carpenter* applies to law enforcement's use of Fog Reveal.[85]

78. *Id.* at 351.
79. *Id.*
80. Burke & Dearen, *supra* note 12.
81. *See id.*
82. *See* H. Brian Holland, *A Third-Party Doctrine for Digital Metadata*, 41 CARDOZO L. REV. 1549, 1558 (2020).
83. *Katz*, 389 U.S. at 351.
84. *See id.*
85. *See Carpenter*, 138 S. Ct. at 2213.

C. The Cell Phone: A Feature of Human Anatomy

Modern cell phones and their services are such "a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[86] The Supreme Court's understanding of the ubiquity of cell phones in modern life was crucial in its Fourth Amendment analysis in *Carpenter*.[87] The fact that cell phones accompany their users almost everywhere they go—twelve percent of smartphone users admit they use their phones in the shower—ensures the intimate nature of the information cell phones store.[88] Indeed, cell phones travel with their owners to private residences, doctor's offices, political headquarters, and other revealing locales.[89] Acknowledging this reality, the Supreme Court in *Carpenter* noted that by tracking a cell phone's location, the government achieves near-perfect surveillance.[90]

Moreover, the Court emphasized the retrospective quality of CSLI.[91] CSLI enables law enforcement to travel back in time to trace a person's location as far back as the wireless carrier's records go, typically five years.[92] This means that when law enforcement identifies a suspect, the suspect has been effectively surveilled for each moment of every day for five years.[93] Another alarming aspect of CSLI is the fact that it could be used against any cell phone user. Because CSLI is "continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone."[94] The privacy concerns presented by CSLI that led the Supreme Court to impose a warrant requirement on its use exist in equal if not greater magnitude by the information captured by Fog Reveal.

While the FBI achieved near-perfect surveillance using CSLI in *Carpenter*, law enforcement agencies achieve even more precise surveillance when using location information from applications like Fog Reveal."[95] When officers obtain an individual's CSLI, they only have access to that individual's information. In contrast, Fog Reveal allows law enforcement to monitor rallies, protests, places of

86. Riley v. California, 573 U.S. 373, 385 (2014).
87. *See Carpenter*, 138 S. Ct. at 2218.
88. *Riley*, 573 U.S. at 395.
89. *See Carpenter*, 138 S. Ct. at 2218.
90. *Id.*
91. *Id.*
92. *Id.*
93. *Id.*
94. *Id.*
95. McKenna, *supra* note 53.

worship, etc.[96] Even though Fog Reveal records location data differently than CSLI—which records when a phone connects to a cell tower—its tracking capabilities are more precise than CSLI.[97]

Furthermore, Fog Reveal presents the same retroactive concerns raised by CSLI. It is inaccurate to think of Fog Reveal as only revealing a person's movements beyond the time they become a person of interest. Indeed, Fog Data Science itself claims to have billions of location data points taken from millions of cell phones.[98] In *Carpenter*, the Supreme Court noted that "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalog every single movement of an individual[] . . . for a very long period."[99] Yet, Fog Reveal provides law enforcement these exact surveillance capabilities. By subscribing to Fog Reveal, law enforcement gains access to the digital trail created whenever a smartphone owner uses an application or visits a website.[100] This information allows law enforcement to establish pattern-of-life profiles on individuals, documenting where they have gone and visited.[101]

Similarly, Fog Reveal, like CSLI, can be used against anyone who owns a cell phone. Again, Fog Data Sciences purports to have billions of data points from over 250 million cellular devices.[102] Accordingly, police need not know in advance whether they want to track or follow a particular individual because the information they may eventually want to discover is harvested by brokers like Fog Reveal and made ready for law enforcement upon request.[103] Given that the information provided by Fog Reveal implicates the same, if not graver, privacy concerns than CSLI, the Supreme Court's holding in *Carpenter* should apply beyond CSLI to cover digital information provided by third-party brokers. For anyone participating in modern society, the cell phone is as much a feature of human anatomy as an arm or a leg; people bring their cell phones with them nearly everywhere they go. This reality cuts against any argument that cell phone users voluntarily relinquish their privacy expectations over the information stored on their mobile devices. In addition, the ubiquity of cell phones in modern life heightens the intimate nature of the information cell phones store. These were the precise concerns that prompted the Supreme Court to recognize a reasonable expectation of privacy over CLSI. Accordingly, the Supreme Court's

96. *Id.*

97. Bennett Cyphers & Aaron Mackey, *Fog Data Science Puts Our Fourth Amendment Rights up for Sale*, ELEC. FRONTIER FOUND. (Aug. 31, 2022), https://www.eff.org/deeplinks/2022/08/fog-data-science-puts-our-fourth-amendment-rights-sale.

98. *Id.*

99. *Carpenter*, 138 S. Ct. at 2217 (citing United States v. Jones, 565 U.S. 400, 430 (2012) (Sotomayor, J., concurring)).

100. McKenna, *supra* note 53.

101. *Id.*

102. *Id.*

103. *See id.*

holding in *Carpenter* should apply to law enforcement's use of software applications like Fog Reveal.

D. Digital Location Data Is Never Anonymous

A principal argument made in support of the government's purchase of location data is that it does not contain any personally identifiable information.[104] In contrast, the FBI in *Carpenter* knew the CSLI it obtained belonged to the Petitioner. Although the location data provided by Fog Reveal is analogous to CSLI in terms of what it reveals, Fog Data Sciences founder Robert Liscouski contends that *Carpenter* does not apply because the data it receives is "hashed and anonymized" before it is turned over to law enforcement.[105]

The "no identifiable information" argument ignores the reality that it is impossible to anonymize location data.[106] Location data reveals unique patterns of movement that make it easy to connect an "anonymous" ID to a real person.[107] A 2013 study involving fifteen months of human mobility data concluded that just four space-time data points were needed to identify ninety-five percent of individuals.[108] Were this not the case, it is unclear why law enforcement would even want access to the troves of location information collected by Fog Reveal in the first place. Moreover, analysts who use the data attest to the ease with which the device owners can be tracked.[109]

After dispensing with the "anonymized" information argument, it is unclear how else to distinguish the FBI's use of CSLI in *Carpenter* from law enforcement's purchase of location information from data brokers. Both implicate the same privacy concerns because both CSLI and location information reveal a person's physical movements and, thus, the places they visit and with whom they associate.[110] When law enforcement obtains location information through brokers like Fog Reveal, it does not know the person's identity until it has access to the data, but the result is the same. Because the data supplied by Fog Reveal and other brokers disclose the intimate details of a person's life that can be used to identify that person, location data is analogous to CSLI; thus, *Carpenter* requires law enforcement to obtain a warrant before purchasing digital location information.

---

104. Cyphers & Mackey, *supra* note 97.
105. *Id.*
106. *Id.*
107. *Id.*
108. Montjoye et al., *supra* note 63, at 1.
109. Matsuoka, *supra* note 1.
110. Bennett Cyphers, *How the Federal Government Buys Our Cell Phone Location Data*, ELEC. FRONTIER FOUND. (Jun. 13, 2022), https://www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data; Robinson Meyer, *This Very Common Cellphone Surveillance Still Doesn't Require a Warrant*, THE ATLANTIC (Apr. 14, 2016), https://www.theatlantic.com/technology/archive/2016/04/sixth-circuit-cellphone-tracking-csli-warrant/478197.

E. Location Data and The Risk of Discrimination

Not only does the government's use of location data broadly threaten the privacy of everyday Americans, but its use may also lead to discrimination against marginalized communities. In 2020, the U.S. military purchased location data from two companies called Babel Street and X-Mode that, themselves, pay apps to harvest location data that it can sell.[111] Most of the data purchased by the U.S. military came from Muslim Pro, a Muslim prayer and Quran app that has more than ninety-eight million downloads worldwide.[112] After the story broke, the American Civil Liberties Union filed a Freedom of Information Act request against the U.S. government seeking the release of three years of records, alleging that the data purchases "discriminate against Muslims and violate the Fourth Amendment[]. . . ."[113]

The U.S. military's decision to target the location data of Muslims demonstrates how the use of cellular location data can be used to monitor specific communities. Unlike CSLI, which is limited to the physical movements of a specific individual, when the government contracts with data brokers like Fog Data Sciences and Babel Street, it gains access to the location data of every device within a specified area.[114] For instance, a government agency with access to Fog Reveal can log into the application to see a map.[115] It can then outline a specified area, add a time frame, and Fog Reveal "spit[s] out all of the mobile device ids within that time frame and location."[116] This capability gives the government the ability to monitor particular communities and to surveil political organizations and protests.

For example, in June 2020, Mobilewalla, a data broker that purchases phone data from apps installed on phones, published a report detailing the race, age, gender, and religion of individuals who participated in the Black Lives Matter protests during the weekend following George Floyd's killing.[117] "None of [the protesters] being tracked had any idea at the time, nor do they know now," according to Mobilewalla.[118] Essentially, the U.S. government now has access to

111. Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, VICE (Nov. 16, 2020, 10:35 AM), https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.

112. *Id.*

113. Gabrielle Canon, *ACLU Files Request Over Data US Collected via Muslim App Used by Millions*, THE GUARDIAN (Dec. 3, 2020, 4:34 PM), https://www.theguardian.com/us-news/2020/dec/03/aclu-seeks-release-records-data-us-collected-via-muslim-app-used-millions.

114. Dahan, *supra* note 58.

115. Matsuoka, *supra* note 1.

116. *Id.*

117. Zak Doffman, *Black Lives Matters: U.S. Protesters Tracked by Secretive Phone Location Technology,* FORBES (June 26, 2020, 11:22 AM), https://www.forbes.com/sites/zakdoffman/2020/06/26/secretive-phone-tracking-company-publishes-location-data-on-black-lives-matter-protesters/?sh=a8912bf4a1ea.

118. *Id.*

a tool that allows it to monitor and disrupt political movements.[119] It is obvious why law enforcement might be tempted to use Fog Reveal to monitor individuals who are speaking out against the police. Another frightening implication of the government's newfound surveillance power comes from the Supreme Court's decision in *Dobbs*.[120] Law enforcement agencies may eventually use Fog Reveal to outline abortion clinics and track the patients seeking healthcare.[121] Although social activism related to police brutality and reproductive rights are the most salient issues at present, there is a risk that location data will be used against any political movement that draws the government's ire.

IV. SOLUTIONS

A. Options Available to The Judiciary

Until Congress passes a comprehensive data privacy law, the judiciary has two options to prevent law enforcement from evading the Fourth Amendment's warrant requirement by purchasing location information from data brokers: (1) lower courts must interpret *Carpenter* to require law enforcement to obtain a warrant before purchasing data that records an individual's physical movements; or (2) the Supreme Court should hear a case involving the government's purchase of location information and the subsequent use of that information in a criminal investigation.

The first option is the most practical solution available to the judiciary because it is a response that can be implemented immediately. Lower federal courts have far less power to decide the cases they hear, as opposed to the Supreme Court. Typically, the Supreme Court hears an issue only after it has been decided in the United States Court of Appeals or the highest Court in a given state.[122] Additionally, four of the nine Justices must vote to accept a case.[123] While waiting for the Supreme Court to clarify its holding in *Carpenter*, lower courts should read *Carpenter* to require law enforcement to obtain a warrant before purchasing location information. Specifically, lower courts must acknowledge that the *Carpenter* holding was based on the Court's concern with the

119. *Feds Deliberately Targeted BLM Protesters to Disrupt the Movement, a Report Says*, NPR (Aug. 20, 2021, 9:10 AM), https://www.npr.org/2021/08/20/1029625793/black-lives-matter-protesters-targeted.

120. *See generally* Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228 (2022).

121. Matthew Guariglia. *Members of Congress Urge FTC to Investigate Fog Data Science*, ELEC. FRONTIER FOUND. (Sept. 15, 2022), https://www.eff.org/deeplinks/2022/09/members-congress-urge-ftc-investigate-fog-data-science.

122. *Supreme Court Procedures*, UNITED STATES CTS., https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/supreme-1(last visited Aug. 28, 2023).

123. *Id.*

intimate nature of the information provided by CSLI.[124] The FBI's acquisition of CSLI was a search, not because CSLI was obtained through a compulsory legal process, but because CSLI reveals a detailed history of an individual's physical movements.[125] Lower courts can close the "Data Broker Loophole" argument by clarifying that the sensitive nature of digital location information will implicate the Fourth Amendment regardless of whether it is obtained through purchase or compulsory legal process. By interpreting *Carpenter* in this way, lower courts will minimize the risk of Fourth Amendment violations against American citizens until Congress or the Supreme Court decides to act.

Lower courts requiring law enforcement agencies to obtain a warrant before accessing an individual's personal location information is a temporary solution. For American citizens to have robust privacy protections over the digital data that reveals their physical movements, the Supreme Court must act. To give American citizens certainty over their privacy expectations, the Supreme Court must clarify how the Fourth Amendment applies to third-party government data purchases. Accordingly, the Supreme Court must hear a case involving the warrantless purchase of digital location information from private third-party brokers and permanently close the "Data Broker Loophole." To close the loophole, the Court must categorically acknowledge that American citizens have a reasonable expectation of privacy over the physical record of their physical movements.[126] Further, the Court must acknowledge that the reasonable expectation of privacy over information endures regardless of how the information is obtained—save for extraordinary circumstances like consent or voluntary disclosure.

B. Options Available to The Legislature

The most robust solution is for Congress to pass legislation closing the third-party broker loophole. Passing a comprehensive federal data privacy law is the most obvious solution, but such a solution has proved untenable.[127] The proposal of the American Data Privacy and Protection Act was a step in the right direction, but

124. *See Carpenter*, 138 S. Ct. at 2217 (explaining that an individual expects privacy in daily movement and so it requires protection, with the intimate nature of that tracking data being critical to that decision).

125. *Id.* (noting that CSLI data provides a "detailed and comprehensive" history of an individual's movements).

126. *Id.*

127. *See, e.g.*, Nick Sibilia, *Congress Could Soon Ban Police from Buying Your Data Without a Warrant*, FORBES (Aug. 1, 2023, 8:00 PM), https://www.forbes.com/sites/nicksibilla/2023/08/01/congress-could-soon-ban-police-from-buying-your-data-without-a-warrant/?sh=4b3aabfc5171 (noting that Congress is attempting to deal with the issue presented by CSLI and addressed in *Carpenter* with comprehensive legislation, but also that this is the second time the bill has been introduced, so the bill passing could be unlikely).

neither the Senate nor the House of Representatives had time to consider the proposal before the conclusion of the 117th Congress.[128] Moreover, Congress has tried, unsuccessfully, for over twenty years to pass a federal privacy law, creating skepticism that it will ever succeed.[129] If Congress does pass a comprehensive federal data privacy law, it should model the General Data Protection Regulation ("GDPR") that applies to members of the European Union.[130] The GDPR requires data subjects to give explicit consent before their data is collected.[131] Such a requirement would alleviate the concerns posed by software applications like Fog Reveal.

Despite the infeasibility of Congress passing a comprehensive federal data privacy act anytime soon, Congress should exhaust its more practical options. The first is an amendment to the ECPA closing the third-party broker loophole. The ECPA should be amended to restrict private third parties who obtain customer information from ECS and RCS providers from selling that information to the government. This might require third parties who purchase data from ECS and RCS providers to be designated as a particular entity within the Act that is prohibited from selling information from the government.

Another option that would alleviate some of the concerns over the government's purchase of location information is to regulate the anonymization techniques used by third-party brokers. If, for instance, the location information Fog Reveal provided to law enforcement were truly anonymous and incapable of being traced to a person, there would be fewer privacy concerns. Law enforcement would merely have access to the digital information of an anonymous phone ID rather than a real person. Of course, this solution is predicated on the advancements of anonymization technology given how difficult it is to anonymize location information.

Aside from ensuring privacy protections via a federal data privacy law, closing the third-party broker loophole must be Congress's priority. As mentioned above, Congress could close this loophole by amending existing laws or by regulating data brokers. These are more practical options that could be implemented with greater ease than passing a federal law but would still create meaningful privacy protections for American citizens.

---

128. *The American Data Privacy and Protection Act*, A.B.A. (Aug. 30, 2022), https://www.americanbar.org/advocacy/governmental_legislative_work/publications/washingtonletter/august-22-wl/data-privacy-0822wl.

129. Jessica Rich, *After 20 Years of Debate, It's Time for Congress to Pass a Baseline Poverty Law*, BROOKINGS (Jan. 14, 2021), https://www.brookings.edu/blog/techtank/2021/01/14/after-20-years-of-debate-its-time-for-congress-to-finally-pass-a-baseline-privacy-law.

130. *See* Osano Staff, *Data Privacy Laws: What You Need to Know in 2023*, OSANO (Dec. 14, 2022), https://www.osano.com/articles/data-privacy-law (explaining that GDPR applies to the EU member countries).

131. *Id.*

V. CONCLUSION

The Supreme Court's Fourth Amendment jurisprudence should keep pace with the rapid advancements of technology. When the Fourth Amendment was drafted, the primary, if not the only, way for the government to intrude into the private affairs of a citizen was to enter the individual's home forcibly. In 2023, the government possesses an unknown number of surveillance tools allowing it to learn the intimate details of an individual's life without ever alerting the individual under surveillance.[132] To preserve the privacy protections the Fourth Amendment offers, the Court and the legislature must recognize the myriad new ways the government can intrude into citizens' private affairs and react accordingly.[133]

To ensure that the protections of the Fourth Amendment are as robust as they were at its drafting, the Supreme Court must require government agencies to obtain a warrant before purchasing location data from third-party brokers.

132. *See Carpenter*, 138 S. Ct. at 2219 (noting that modern targets of surveillance are not alerted to it).

133. *See, e.g.*, Noah Chauvin, *New Legislation Would Close a Fourth Amendment Loophole*, BRENNAN CTR. FOR JUST. (July 6, 2023), https://www.brennancenter.org/our-work/analysis-opinion/new-legislation-would-close-fourth-amendment-loophole (explaining how the current state of electronic surveillance has created a Fourth Amendment issue that needs to be solved by comprehensive legislation).