Note

An (Un)reasonable Expectation of Privacy? Analysis of the Fourth Amendment When Applied to Keyword Search Warrants

*Helen Winters**

INTRODUCTION

In the recent R. Kelly racketeering and sexual exploitation case,[1] a car belonging to an outspoken victim of the star was set on fire.[2] To find the culprit, Google disclosed to a federal agent the Internet Protocol (IP) addresses of those who used its search engine to find the victim's address. Law enforcement used this data to identify Michael Williams, an associate of the accused musician, who was then proven to have set fire to the car.[3] Google's actions were widely criticized by experts, such as the surveillance and cybersecurity counsel of the ACLU, citing concern for the precedent set by such warrants and the potential for a breach of the Fourth Amendment.[4] Others have critiqued

* J.D. Candidate 2023, University of Minnesota Law School; Note & Comment Editor, *Minnesota Law Review* Vol. 107. I am forever grateful to Professor Maria Ponomarenko for her invaluable guidance in developing this Note; to the editors and staff on *Minnesota Law Review* for their diligience and thoughtful feedback in publishing this piece; to my brilliant peers for their endless support inside and outside of the classroom; and to my family for always picking up the phone.

1. *See, e.g.*, Siladitya Ray, *Google Shared Search Data with Feds Investigating R. Kelly Victim Intimidation Case*, FORBES (Oct. 9, 2020), https://www.forbes.com/sites/siladityaray/2020/10/08/google-shared-search-data-with-feds-investigating-r-kelly-victim-intimidation-case/?sh=341140e97c62 [https://perma.cc/649A-7BNS].

2. *See* Alfred Ng, *Google Is Giving Data to Police Based on Search Keywords, Court Docs Show*, CNET (Oct. 8, 2020), https://www.cnet.com/tech/services-and-software/google-is-giving-data-to-police-based-on-search-keywords-court-docs-show [https://perma.cc/8DE7-54XR].

3. *Id.*

4. *See* Thomas Brewster, *Exclusive: Government Secretly Orders Google to Identify Anyone Who Searched a Sexual Assault Victim's Name, Address, or Telephone Number*, FORBES (Oct. 4, 2021), https://www.forbes.com/sites/

Google's stored data system itself, suggesting the company could do more to protect users' privacy. As the Electronic Frontier Foundation's surveillance litigation director stated, "[i]f Google stored data in a way that was truly de-identified, then they also couldn't give it to the government. Google's not setting up their system or changing their practices in a way that could prevent these kinds of searches."[5] Numerous news outlets have spoken out seemingly opposed to the current practice, representing the public's concern over personal privacy.[6] This case highlights the rise in usage of technology-based search warrants, and has strong implications for the future of Fourth Amendment jurisprudence.

Keyword search warrants are a type of reverse search warrant by which law enforcement seeks information that can be used to create a pool of suspects for investigation.[7] With a keyword search warrant, the police ask search engine companies like Google for detailed information of any internet user who has used a specific search term, or "keyword." For example, in the above R. Kelly case, the police asked Google for data on any "user[] who had searched the address of the residence close in time to the arson."[8] Google then sent a list of IP addresses that had searched for the arson victim's address to law enforcement.[9]

---

thomasbrewster/2021/10/04/google-keyword-warrants-give-us-government-data-on-search-users/?sh=26ebc5e17c97 [https://perma.cc/WKY5-QVW5].

5. Ng, *supra* note 2.

6. *See, e.g.*, Ray, *supra* note 1 (writing for Forbes); Ng, *supra* note 2 (writing for CNET); Isobel Asher Hamilton, *Documents from an Arson Attack Linked to the R Kelly Investigation Show How Google Hands "Keyword" Search Data to Police*, BUS. INSIDER (Oct. 9, 2020), https://www.businessinsider.com/google-can-give-police-keyword-data-from-search-histories-2020-10 [https://perma.cc/VPT8-6DEF].

7. Albert Fox Cahn & Amanda Humell, *"Keyword Warrants" Make Every Search a Risk: A Disturbing New Police Tactic Harnesses the Full Tracking Power of "Big Tech"*, VERFASSUNGSBLOG (Oct. 15, 2020), https://verfassungsblog.de/keyword-warrants [https://perma.cc/CZX7-G637].

8. Hamilton, *supra* note 6; *see* Affidavit in Support of an Application for a Search Warrant at 7–9, *In re* The Search of Information Associated with the Cellular Device Assigned Call Number (229) 418-8231, That Is Stored at Premises Controlled by T-Mobile, No. 20-MC-1584 (E.D.N.Y. July 13, 2020). While this Affidavit does not include the search warrant itself, it does reference what was authorized. However, little public information exists to determine how close the search needed to be to the time of arson.

9. Hamilton, *supra* note 6; *see also* Affidavit in Support of an Application for a Search Warrant, *supra* note 8, at 7–8.

Two of these IP addresses were linked to Williams's phone number, which was then used to track the phone's location at the time of the crime.[10] This information corroborated that the device was near the victim's car at the time of the arson attack.[11] Investigators were then able to establish particularity and probable cause necessary to obtain a warrant for Williams's personal search history, which showed searches for "where can i [sic] buy a .50 custom machine gun," "witness intimidation," and "countries that don't have extradition with the United States."[12]

The process of obtaining a reverse warrant is not fixed, but generally involves two to three steps.[13] First, the government requests internet or cellular providers search their databases to produce a list of the accounts who have searched the listed terms.[14] In some cases, warrants ask for account information at this stage; in others, this is given at a later stage.[15] Next, law enforcement reviews the list and determines the users they are interested in.[16] If law enforcement has not yet accessed personal identifying information, they then file a second warrant for this information. Finally, law enforcement may issue an individual-specific warrant for those that have been identified with the information from search providers.[17] This can then be used to obtain an individualized search warrant to investigate data associated with the suspect's personal devices, as was the case with Williams.[18]

Rather than initially seeking information for an individual suspect, police use this type of "reverse search warrant" to

---

10. Hamilton, *supra* note 6.

11. *Id.*

12. *Id.*

13. Google has not come out with a list of steps. However, Google has released the process in a general two or three-step progression for analogous geofence warrants. The process for a keyword warrant is similar, and this was used as a template for the keyword warrant process in this Note. Additionally, warrants referenced throughout utilize the same framework, and thus are corroborated. *See* Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from a "Geofence" General Warrant at 12–14, United States v. Chatrie, No. 19-cr-00130-MHL (E.D. Va. Dec. 20, 2019) [hereinafter Google Amicus Brief].

14. *Id.* at 12.

15. *Id.* at 3.

16. *Id.* at 13–14.

17. *See id.* at 2–3, 14; *see also* Hamilton, *supra* note 6.

18. Affidavit in Support of an Application for a Search Warrant, *supra* note 8, at 7–8.

gather information on an unrestricted number of users who fit the parameters from which they choose potential suspects.[19] These searches may be direct—for example, by having Google directly disclose the IP addresses of those who searched for a particular term—or may be indirectly conducted through third-party apps linked to Google services.[20] In some cases, like the R. Kelly case, these IP addresses are used to confirm a potential suspect or known associate of a person of interest; in other cases, it is the first step in compiling a list of potential suspects.[21]

In order to access information given to online service providers such as Google, law enforcement relies upon the third-party doctrine.[22] This doctrine states that individuals have no legitimate expectation of privacy for information that is voluntarily shared with third parties, regardless of whether they intended for the government to have access to this data, such as bank papers and phone records.[23] This principle has broad implications: law enforcement can obtain a set of papers from a third party with whom they have been shared, wheras a warrant would otherwise be needed to obtain them from the home, with little to no constitutional repercussions.[24]

---

19. Johana Bhuiyan, *The New Warrant: How U.S. Police Mine Google for Your Location and Search History*, GUARDIAN (Sept. 16, 2021), https://www.theguardian.com/us-news/2021/sep/16/geofence-warrants-reverse-search-warrants-police-google [https://perma.cc/JM9S-LCQ3]; *see also* Affidavit in Support of an Application for a Search Warrant, *supra* note 8, at 7–8 (showing the lack of numerical limit on the number of subjects to be turned over in response to the requested search parameters in this case).

20. *See, e.g.*, Kim Lyons, *Google Location Data Turned a Random Biker into a Burglary Suspect*, VERGE (Mar. 7, 2020), https://www.theverge.com/2020/3/7/21169533/florida-google-runkeeper-geofence-police-privacy [https://perma.cc/3HMU-UU7T] (describing the case of a Florida man who was implicated in a burglary by a geofence warrant using data collected from his RunKeeper app, which placed him at the scene of a crime he was unaware had occurred).

21. *See* Hamilton, *supra* note 6.

22. *See infra* Part I.A.2 (discussing the third-party doctrine and its implications in the digital age).

23. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 744 (1979) (discussing privacy expectations in phone records); United States v. Miller, 425 U.S. 435, 442–44 (1976) (discussing privacy expectations in bank papers).

24. Given the constitutional limits, Congress has responded with regulations to protect individual data and promote data privacy. However, there is no comprehensive statutory scheme regulating third party usage of data. *See, e.g.*, STEPHEN P. MULLIGAN & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., IF11207, DATA PROTECTION AND PRIVACY LAW: AN INTRODUCTION (2022), https://crsreports.congress.gov/product/pdf/IF/IF11207 [https://perma.cc/3LXV-QZLZ].

As Justice Sonia Sotomayor opined in her concurrence in *Jones*, existing Fourth Amendment jurisprudence is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[25] The Court confronted such critiques, although not exhaustively, in *Carpenter*. In its decision, the Supreme Court diverged from the third-party doctrine to reconsider what constitutes a reasonable expectation of privacy in the digital age. The *Carpenter* Court held that certain types of personal data-based searches constitute Fourth Amendment protected searches, and therefore require a valid warrant instead of falling under the third-party doctrine exception.[26]

Like geofence warrants, a similar reverse search warrant technique utilizing technology to conduct searches of personal devices located near a specific area at a given time,[27] a keyword search warrant implicates the Fourth Amendment and perceptions of what a reasonable expectations of privacy entails. In particular, the use of reverse warrants raises the question of what privacy rights exist in information given to online service providers, such as Google.[28] Such warrants prompt new questions as to the type of information the government may freely access, and what privacy protections an individual—or a pool of individuals—may reasonably be expected to have.[29] While open-ended electronic search tools can aid law enforcement in solving otherwise difficult cases, they may also implicate innocent persons,[30] and allow law enforcement access to broad caches of personal in-

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

26. Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018).

27. Bhuiyan, *supra* note 19.

28. *See* U.S. CONST. amend. IV (protecting from unreasonable searches and seizures by the government and specifying probable cause and particularity as warrant requirements); *see also* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); *Smith*, 442 U.S. at 742 (demonstrating that individuals have no reasonable expectations of privacy in information they voluntarily provide to third parties). These questions have not yet been comprehensively analyzed regarding keyword search warrants and their data collection.

29. *See, e.g.*, Jessica F. Silva, *Reasonable Expectations of Privacy in the Digital Age*, 44 SETON HALL LEGIS. J. 607 (2019) (analyzing the application of the Fourth Amendment to digital privacy and criticizing today's protections).

30. Lyons, *supra* note 20.

formation. For these reasons, it is important for courts to be cautious about their extension of the third-party doctrine to the technological era.

This Note contributes to existing literature by showcasing how existing Fourth Amendment jurisprudence leaves a hole in privacy protections, particularly for data attached to personal data other than cell-site location information (CSLI). Part I discusses historical Fourth Amendment jurisprudence, focusing on what investigation techniques have been considered violative in the face of technological advancement. Part II gives a brief overview of the reverse keyword search technique and evolving personal privacy expectations. Part III suggests that the *Carpenter* decision and subsequent caselaw, although groundbreaking, do not properly respond to our society's technological realities.[31] Finally, Part IV address rising calls for legislative action, and why going beyond the judiciary may be the best solution. While keyword search warrant techniques and other reverse techniques are likely Fourth Amendment searches, they are protected under the third-party doctrine. This Note finds that a hole in protection exists, and a legislative solution should be considered.

I. IS IT A SEARCH? ANALYZING FOURTH AMENDMENT JURISPRUDENCE

The caselaw surrounding the Fourth Amendment is often convoluted and fact-specific, utilizing tools such as an inside/outside distinction[32] and physical limitations on privacy.[33] These nuances were created for a less advanced society, and thus have limitations in their application to electronic data.[34] The zone of Fourth Amendment protection has ebbed and flowed under the

31. *See* U.S. CONST. amend. IV; *Carpenter*, 138 S. Ct.

32. *Katz*, 389 U.S. at 361 (Harlan, J., concurring) ("[C]onversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable."). However, entering ordinarily enclosed spaces constitutes a search. *See, e.g.*, Olmstead v. United States, 277 U.S. 438 (1928) (utilizing the physical trespass doctrine).

33. Physical scale often limits how far searches can go: a search incident to arrest includes the physically grabbable area near the arrestee, but generally no further. *See, e.g.*, New York v. Belton, 453 U.S. 454, 460 (1981).

34. Josh Daniels, *Protecting the 4th Amendment in the Digital Age*, LIBERTAS INST. (Mar. 25, 2014) https://libertas.org/personal-freedom/protecting-the-4th-amendment-in-the-digital-age [https://perma.cc/5QZD-WJSM] ("The [F]ounders did not have cell phones and could not have imagined all of the technology of our digital age.").

trespass doctrine[35] and the reasonable expectation of privacy test,[36] with considerable exception for data privacy given to third parties.[37] The *Carpenter* decision challenged this precedent, signaling growing concern for adaptation of existing doctrine to reflect society's changing expectations of digital privacy.[38] Such adaptation may plausibly be extended to data obtained under keyword search warrants, with limitations.[39]

A. THE INFLUENCE OF TECHNOLOGY ON THE FOURTH AMENDMENT'S APPLICATION

The Fourth Amendment requires all searches and seizures to be reasonable.[40] Ordinarily, this requires a warrant supported by probable cause.[41] As the Fourth Amendment only applies to searches and seizures, much turns on whether an investigative technique constitutes a Fourth Amendment "search": where a governmental actor violates an individual's reasonable expectation of privacy, the actor is conducting a search and would thus be required to obtain a warrant.[42] However, the warrant does not have to show that the suspect's criminal activity is more likely true than false; this is often referred to as a "reasonableness" and "totality of the circumstances" test.[43] Once probable cause

35. *See Olmstead*, 277 U.S. at 466; *infra* Part I.A.1.

36. *See Katz*, 389 U.S. at 349–51; *infra* Part I.A.1.

37. This is referred to as the third-party doctrine. *See infra* Part I.A.2.

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

39. *See infra* Part III.

40. *See* 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 . . . .").

41. Warrants must be issued only upon probable cause and particularity in describing the place to be searched and the items seized. *See* Boyd v. United States, 116 U.S. 616, 625–26 (1886) (detailing the history of how general warrants came to be unconstitutional).

42. *Id.*

43. Probable cause is a flexible concept, requiring a judge to weigh the totality of information presented to decide if there is a fair probability that the search will expose particular evidence of a crime. *See* Illinois v. Gates, 462 U.S. 213, 240 (1983) (characterizing a judge's probable cause as "the essential protection of the warrant requirement."). *But see* Omelas v. United States, 517 U.S. 690, 695–96 (1996) (stating it is impossible to provide a precise articulation of the meaning of probable cause); *Gates*, 462 U.S. at 241 (conceding that the probable cause test is "not technical") (internal citation omitted). Law enforcement must demonstrate more than a mere suspicion, but it does not have to meet the higher preponderance of the evidence standard.

exists, a court turns to particularity.[44] Historically, the Supreme Court has interpreted the Fourth Amendment as extending the expectation of privacy to the home alone.[45] In *Katz*, the Court extended the amendment's protection to surveillance beyond the home, promulgating the "reasonable" expectation of privacy test.[46] This test has been cabined by the third-party doctrine, suggesting there are some types of data where an individual does not have a reasonable expectation of privacy protection.[47] The limits of such a doctrine are tested, although not conclusively, in *Carpenter*.

1. From *Olmstead* to *Katz*: Where Is One Protected from a Search?

Early decisions regarding the Fourth Amendment extended protections exclusively to tangible material effects, or *physical* invasions, of persons, houses, papers, and effects.[48] A person's home receives the highest level of Fourth Amendment protection, founded on the historical belief that the home is the most private of places.[49] The goal of protecting the home is to protect the "privacies of life," including intimate and private details of a person's day.[50] Notably, this distinction was crafted where technology was lacking. However, interpretation of what should be granted such sanctity has evolved, expanding from the *Olmstead* physical trespass doctrine to the much broader *Katz* reasonable expectation of privacy. While initially expansive, the reasonable

44. *See* Maryland v. Garrison, 480 U.S. 79, 88–89 (1986) (holding the police made "reasonable effort to ascertain and identify" the place to be searched); Steele v. United States, 267 U.S. 498, 503 (1925) (stating the description should allow the police officer to easily find the place to be searched); s*ee also* United States v. Grubbs, 547 U.S. 90, 97 (2006) (stating that the Fourth requires two particularized descriptions); Marron v. United States, 275 U.S. 192, 196 (1927) (stating that particularized descriptions of the things to be seized prevent the police from exceeding the scope of the warrant).

45. Olmstead v. United States, 277 U.S. 438, 466 (1928).

46. *See* Katz v. United States, 389 U.S. 347, 349–51 (1967).

47. *Infra* Part 1.A.2.

48. *See, e.g.*, *Olmstead*, 277 U.S. at 466 (solidifying the physical trespass doctrine discussed below).

49. *See* Boyd v. United States, 116 U.S. 616, 630 (1886) (declaring the Fourth Amendment to protect the sanctity of a person's home and the "privacies of life" therein contained); s*ee also* Stephanie M. Stern, *The Inviolate Home: Housing Exceptionalism in the Fourth Amendment*, 95 CORNELL L. REV. 905, 912 (2010) (describing the level of highest protection awarded to homes).

50. *Boyd*, 116 U.S. at 630.

expectation of privacy has been pared down as the courts have encountered the digital age.

Historically, a Fourth Amendment violation required a "physical trespass," and thus limited what could be considered constitutionally protected. This "trespass doctrine" first appeared in *Olmstead v. United States*.[51] In *Olmstead*, the Supreme Court considered whether wiretapping by federal officers of an individual's phone calls was an illegal search under the Fourth Amendment. The Court turned to the Fourth Amendment's historical purpose, "to prevent the use of governmental force to search a man's house, his person, his papers, and his effects, and to prevent their seizure against his will."[52] Emphasis was placed not on the materiality of the violation, but on the fact that there was no "physical trespass," and consequently no illegal search.[53] The *Olmstead* Court warned against attributing such an expansive meaning to the Fourth Amendment; however, Justice Brandeis's dissent advised that "time works changes, brings into existence new conditions and purposes," and thus the law should adapt to these "subtler and more far-reaching means of invading privacy" now available to the government.[54] The *Olmstead* decision was not substantively challenged, and the trespass doctrine guided Fourth Amendment jurisprudence, until *Katz*.

In *Katz v. United States*, the petitioner was convicted with transmitting wagering information by telephone. The FBI obtained evidence of the phone call by attaching an electronic listening device to the public telephone booth the petitioner made the phone call from.[55] The booth was transparent, and thus the Government stressed that Katz was just as visible inside the

51. 277 U.S. 438 (1928).

52. *Id.* at 463; *see also id.* at 464–67 (holding that no Fourth Amendment violation occurs when the government wire taps a defendant's phone without a warrant). The Court held that, under *Carroll v. United States*, 267 U.S. 132, 149 (1925), the Fourth Amendment is to be construed in the light of what was deemed an unreasonable search and seizure at the time it was adopted. While the Fourth Amendment is to be liberally construed in the interest of liberty, the *Olmstead* Court believed it "cannot justify enlargement of the language employed beyond the possible practice meaning of houses, persons, papers and effects" to effectively forbid hearing or sight. *Olmstead*, 277 U.S. at 465.

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

54. *Id.* at 473.

55. 389 U.S. 347, 348–49 (1967).

booth as if he had remained outside.[56] Further, the listening device did not pierce the phone booth, thereby passing the trespass doctrine's test.[57] However, the Court disregarded this argument because Katz sought to exclude the uninvited ear when entering the phone booth rather than the intruding eye.[58] While the Court of Appeals for the Ninth Circuit rejected the contention that the recording was a violation of the Fourth Amendment,[59] the Supreme Court declined to adopt the trespass doctrine to protect the FBI's conduct.

Instead, the Court held that although the Fourth Amendment "cannot be translated into a general constitutional 'right to privacy,'" it still protects a variety of individual privacies from certain kinds of governmental intrusions of privacy.[60] While "the absence of such [physical] penetration was at one time thought to foreclose further Fourth Amendment inquiry," the *Katz* Court found the premise that property interests control the right of the Government to search and seize has and should be discredited.[61] As the majority opinion wrote, "the Fourth Amendment protects people, not places."[62] In *Katz*, the Court stressed the "vital role" that the public telephone had come to play in private communication, emphasizing the need for the amendment to adapt to modern technologies as activities like phone calls began to take place in semi-public and public places.[63] This complicated the importance of the home as the essence of physicality, and thus signaled the need for broader construction.[64]

---

56. *Id.* at 352.

57. *Id.* ("[T]he surveillance technique involved no physical penetration of the telephone booth from which the petitioner placed his calls. It is true that the absence of such penetration was at one time thought to foreclose further Fourth Amendment inquiry.").

58. *Id.* at 353 ("Indeed, we have expressly held that the Fourth Amendment governs not only the seizure of tangible items but extends as well to the recording of oral statements overheard without any 'technical trespass under . . . local property law.'").

59. Katz v. United States, 369 F.2d 130 (9th Cir. 1966).

60. *Katz*, 389 U.S. at 349–51.

61. *Id.* at 352–53.

62. *Id.* at 351.

63. *Id.* at 352.

64. *Id.* at 352–53 ("[A]lthough a closely divided court supposed . . . that surveillance without any trespass and any seizure of any material object fell outside the ambit of the Constitution, we have since departed from [that] narrow view . . . .").

The *Katz* decision changed the standard of analysis to a general reasonable expectation of privacy and expanded Fourth Amendment coverage to non-physical surveillance. Further, it began to extend protection against the invasion of modern technological privacies.[65] Instead of focusing solely on property interests to determine whether or not a "search" has occurred, the Court broadened the scope of protection to any activity in which society is prepared to find a reasonable privacy expectation.[66] Under *Katz*, two prongs must be satisfied: (1) "that a person [has] exhibited an actual (subjective) expectation of privacy," and (2) "that the expectation [is] one that society is prepared to recognize as 'reasonable.'"[67] This reasonableness standard is often the prong at issue in today's cases.

2. The Third-Party Doctrine and the Digital Age

In addition to the *Katz* reasonableness factor,[68] the Court went on to distinguish what *kind* of information is protected from certain parties. In *United States v. Miller* and *Smith v. Maryland*, the Court promulgated the third-party doctrine, which states that individuals have no legitimate expectation of privacy for information that is voluntarily shared with third parties, regardless of whether they intended for the government to have access to this data.[69] The implication of such a premise is extremely broad: under the third-party doctrine, law enforcement could obtain data an individual has shared with a third party with little to no constitutional repercussions, whereas a warrant would be needed to obtain the same data from an individual's home.[70]

---

65. *See id.* at 353 ("[O]nce it is recognized that the Fourth Amendment protects against people—and not simply 'areas'—against unreasonable searches and seizures it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.").

66. *Id.* at 351–54 (discussing the Court's turn away from the historical physical trespass doctrine: "[w]e conclude that the underpinnings of *Olmstead* . . . have been so eroded by our subsequent decisions that the trespass doctrine there enunciated can no longer be regarded as controlling.").

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

68. *See supra* notes 64–66 and accompanying text (discussing the Court's decision in *Katz*, which extended the scope of Fourth Amendment coverage).

69. United States v. Miller, 425 U.S. 435, 442–44 (1976); Smith v. Maryland, 442 U.S. 735, 744 (1979).

70. Given the constitutional limits, Congress has responded with regulations to protect individual data and promote data privacy. However, there is no

In *Miller*, the Court held that the defendant had no legitimate expectation of privacy in his financial records, including copies of checks and deposit slips maintained by his bank, because he had voluntarily conveyed the information to the third-party bank.[71] While Miller had shared the records with the bank for the limited and specific purpose of doing business, this limited purpose argument was found irrelevant for the purposes of whether law enforcement needed a search warrant to obtain such records.[72] Similarly, the Court held in *Smith* that the use of a pen register, a device installed to monitor the telephone numbers dialed on defendant's home phone, was not a search requiring a warrant.[73] Use of the phone was seen as an assumption of risk that the phone company may relay numbers called to the authorities, and thus that defendant had no reasonable expectation of privacy in this data.[74]

Dissenting from the *Smith* decision, Justice Marshall opined that "[i]mplicit in the concept of assumption of risk is some notion of choice . . . . By contrast here, unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance."[75] Unlike the Court's decision in *Katz*, in which the Justices unanimously affirmed the decision of the court, Justice Marshall's dissent warned of the implications of such a doctrine on the necessities of modern society.[76] The third-party doctrine continues to control today, although it has begun to lose force in recent years due to its incompatibility with today's technological society.[77]

Many elements relied upon in analysis of Fourth Amendment cases have become increasingly impracticable measures of whether an individual has a reasonable expectation of privacy in

---

comprehensive statutory scheme regulating third party usage of data. *See, e.g.*, MULLIGAN & LINEBAUGH, *supra* note 24.

71. *Miller*, 425 U.S. at 436–37.

72. *Id.* at 437.

73. *Smith*, 442 U.S. at 745–46 ("[P]etitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and . . . even if he did, his expectation was not 'legitimate.' The installation and use of a pen register, consequently, was not a 'search' and no warrant was required.").

74. *Id.* at 744–46.

75. *Id.* at 749–50 (Marshall, J., dissenting).

76. *Id.* at 748–52 (Marshall, J., dissenting).

77. *See infra* Part III (discussing Carpenter v. United States, 138 S. Ct. 2206 (2018), and the decision's potential impact on the future of the Fourth Amendment's interactions with technologies).

their government-sought data.[78] The Court confronted such critique, although not exhaustively, in *Carpenter v. United States*.[79]

B. RECOGNIZING NEW PRIVACY THREATS: THE *CARPENTER* APPROACH

The Supreme Court's decision in *Carpenter v. United States* marked a new period of Fourth Amendment jurisprudence. Narrowing its holding to the facts of the case, the decision illustrates the judiciary's reluctance to uncritically extend the third-party doctrine, and the push to reconsider what constitutes a reasonable expectation of privacy in the digital age.

Based upon CSLI records, defendant Carpenter had been charged with aiding and abetting a series of robberies.[80] CSLI records are automatically generated as cellphones connect to cell towers, and can create a comprehensive picture of a user's location simply from owning the device.[81] Under the Stored Communications Act, the government obtained 12,898 location points to track Carpenter over 127 days from his cellphone carriers.[82] Before trial, Carpenter moved to suppress the CSLI evidence, arguing violation of the Fourth Amendment.[83] The District Court

78. *See, e.g.*, Riley v. California, 573 U.S. 373, 391–93 (2014) ("A conclusion that inspecting the contents on an arestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.").

79. *See infra* Part I.B.

80. *Carpenter*, 138 S. Ct. at 2208–09.

81. Such records are routinely generated when cell phones connect to nearby cell towers at the start and end of phone calls, during transmission of text messages, routine data connections, and several times a minute when the phone is turned on even when not in use. *Id.* at 2211–12 (noting that "[w]hile carriers have long retained CLSI for the start and end of incoming calls, in recent years phone companies have also collected location information from the transmission of text messages and routine data connections."); *see also id.* at 2218 (noting that tracking the location of a cellphone allows the Government to "achieve[] near perfect surveillance, as if it had attached an ankle monitor to the phone's user," which is possible because "location information is continually logged for all of the 400 million devices in the United States . . . ."). This data is currently maintained by wireless carriers for up to five years. *Id.*

82. *Id.* at 2209. *See generally* Stored Communications Act of 1986, 18 U.S.C. § 2703(d) (specifying the requirements for a court order to collect "the contents of a wire or electronic communication, or the records of other information sought").

83. *Carpenter*, 138 S. Ct. at 2209.

denied the motion, and the U.S. Court of Appeals for the Sixth Circuit affirmed.[84]

The case was appealed to the Supreme Court, which reversed and held that acquisition of Carpenter's data constituted an illegal warrantless Fourth Amendment search.[85] However, the Court was careful to limit its holding, declining to explain how it may be applied to other data technologies.[86] Under *Carpenter*, CSLI data is protected by the Fourth Amendment when the police seek seven days or more of such information.[87]

Despite its narrow holding, the *Carpenter* decision is monumental because it moved beyond focusing on the threat posed by technologies not yet in the public use, as it had in the past, to recognize the risk to privacy posed by technologies already commonplace. As the Court opined, "[o]nly the few without cell phones could escape this tireless and absolute surveillance."[88] Further, the Court recognized that the third-party doctrine may be ill suited to such technological realities, and thus the doctrine is not absolute.[89] While the Court did not overturn prior jurisprudence, Chief Justice Roberts recognized that the bright-line rule regarding third-party disclosure is unsuitable as applied to today's societal expectations.[90] Rather, the Court considered whether Carpenter had "truly shared" his CSLI voluntarily, "as

84. *Id.*

85. *Id.* at 2210–11.

86. *Id.* at 2220 ("Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security.").

87. *Id.* at 2217 ("It is sufficient for our purposes today to hold that accessing seven days of CSLI . . . constitutes a Fourth Amendment search.").

88. *Id.* at 2218; *see also* Kyllo v. United States, 533 U.S. 27 (2001) (holding that a search is presumptively unreasonable and subject to Fourth Amendment protection because the technology in question was not in general public use).

89. *Carpenter*, 138 S. Ct. at 2219 ("The Government's position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's . . . .").

90. *Id.* at 2217 ("We decline to extend *Smith* and *Miller* to cover these novel circumstances. Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection.").

one normally understands the term."[91] While some legal scholars have emphasized the narrowness of the *Carpenter* decision, others have maintained that it is a signal of the Court's desire to broaden constitutional protection of individual data.[92]

II. REDEFINING THE SEARCH: THE RISE OF REVERSE SEARCH TECHNIQUES

Part II gives a brief overview of the keyword search technique and evolving reasonable privacy expectations, focusing on the challenges presented by data generated by personal devices. While there are many different ways that keyword warrants have been used, this Note distills the process into two key steps: the production of IP addresses and the production of account information. These two steps are sometimes procedurally combined. Additionally, in some cases, law enforcement officials take a third step of identifying an individual to investigate further. It may take two or three individual requests by law enforcement to get to the individual user from the initial data retrieval.

A. A DIGITAL SOCIETY'S PRIVACY FALLACY

Technology-based warrants have risen in popularity in recent years and are now available in wide variety.[93] They include

91. *Id.* at 2220.

92. *Compare* Barry Friedman, *The Worrisome Future of Policing Technology*, N.Y. TIMES (June 22, 2018), https://www.nytimes.com/2018/06/22/opinion/the-worrisome-future-of-policing-technology.html [https://perma.cc/6Q3E-8VDT] ("The growing use of technology by law enforcement agencies to monitor or target people—particularly people and communities of color—is expanding at head-spinning speed, and nothing the courts do is going to stop that . . . . [The Chief Justice's] opinion didn't overturn the rule that says that any time the government wants information on you that you've provided to a third party, the government can get it, even though in the digital age most of your information is now in the hands of third parties . . . ."), *with* Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 358 (2019) ("*Carpenter* works a series of revolutions in Fourth Amendment law, which are likely to guide the evolution of constitutional privacy in this country for a generation or more.").

93. *See* Laura Hecht-Felella, *The Fourth Amendment in the Digital Age: How* Carpenter *Can Shape Privacy Protections for New Technologies*, BRENNAN CTR. FOR JUST. 12–29 (2021), https://www.brennancenter.org/our-work/policy-solutions/fourth-amendment-digital-age [https://perma.cc/C4Q6-23AX] (surveying how law enforcement may use various surveillance technology including that found in cell phones, smart cars, body-warn technologies, smart doorbells, and web browsers).

warrants based on information from cell site data, location information, text, and call records.[94] These warrants often use data from technologies like cell phones, smart cars, smart homes, personal laptops, and wearable devices.[95] All of these technologies are integral for our modern society, yet invariably create detailed records about our private lives.[96] In some cases, these records are as automatic as the CSLI records at issue in *Carpenter*, and similarly are the product of technologies essential to societal participation.

The literature on the interaction of technology and legal protections is rich and often focused on a personal device lens, such as cellphones or wearable technology.[97] Advances in technology make it so that personal records of banking, email, internet browsing, and cell phone use are "linked and shared more widely and stored for longer than ever before, often without the individual consumer's knowledge or consent."[98]

---

94. *Id.* (applying *Carpenter* logic to these other data types as used in warrants).

95. *See, e.g.*, Brief of Amici Curiae American Civil Liberties Union, American Civil Liberties Union of Georgia, and Riana Pfefferkorn in Support of Appellant Seeking Reversal, Mobley v. State, No. S18G1546 (Ga. May 7, 2019) (arguing that police officers cannot conduct warrantless searches of smart car computers); Christopher Mele, *Bid for Access to Amazon Echo Audio in Murder Case Raises Privacy Concerns*, N.Y. TIMES (Dec. 28, 2016), https://www.nytimes.com/2016/12/28/business/amazon-echo-murder-case-arkansas.html [https://perma.cc/PUK8-8L6J] (discussing use of smart home technology as evidence); Jon Schuppe, *Google Tracked His Bike Ride Past a Burglarized Home. That Made Him a Suspect*, NBC NEWS (Mar. 7, 2020), https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761 [https://perma.cc/CP9K-NYAK] (discussing utilization of smart watch technology in a geofence warrant).

96. *See generally* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004) (detailing how digital technology creates "digital dossiers" of detailed data about an individual through their numerous daily interaction with various technologies).

97. *See, e.g.*, Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805 (2016) (discussing how smart devices interact with the Fourth Amendment); Hecht-Felella, *supra* note 93 (discussing a multitude of technologies but focusing on devices like cellphones and smart watches).

98. Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 456 (2008); *see also* Rebecca Lipman, Note, *The Third Party Exception: Reshaping an Imperfect Doctrine for the Digital Age*, 8 HARV. L. & POL'Y REV. 471, 471–72 (2014) (providing a description of how much and what type of information may be available to third parties based on one's daily online presence).

The majority of Americans see their personal data as less secure than it was five years ago, and more than eight-in-ten Americans are concerned about the amount of personal information collected by companies; in comparison, about six-in-ten Americans are concerned about the government's collection.[99] Clearly, the public has growing concern about data collection and the use of personal data; however, many have not made the connection that companies can work alongside government to utilize their data.

While the value of personal data has increased in recent years, both to the individual and to law enforcement, the law has not progressed in response. Many courts continue to apply the third-party doctrine to these personal data records,[100] under which law enforcement does not need a warrant because the individual "voluntarily" conveys the information to a third party, and thus no illegal search occurs.[101] This allows access to a large aggregate of personal data, a direct concern of the public. The assumption under the doctrine is that information given to third parties is no longer considered "private."

B. THE CHALLENGE OF DEFINING A KEYWORD SEARCH WARRANT

"As with all law enforcement requests," one Google spokesperson states, "we have a rigorous process that is designed to protect the privacy of our users while supporting the important work of law enforcement."[102] While traditional court orders permit searches related to known suspects, keyword search warrants are issued specifically because a suspect cannot be identified.[103] Relatively new to the scene, keyword search warrants are a subset of reverse search warrants that ask internet search providers such as Google, Microsoft, and Yahoo to provide a list of users who have searched for specific terms relevant to an ongoing investigation.[104] Police use this information to narrow down suspects to then investigate further.

---

99. Lipman, *supra* note 98, at 471–72.

100. *See supra* Part I.A.2 (discussing the third-party doctrine's potential applicability to advances in technologies).

101. *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 CALIF. L. REV. 1083, 1085–86 (2002).

102. *See* Brewster, *supra* note 4.

103. *Id.*

104. *See, e.g.*, Affidavit at 1–2, *In re* The Search of Information and Records Associated with Google Searches for Various Search Terms That Are Stored at

For example, investigators in the aforementioned R. Kelly case were able to tie Williams to arson through the keyword warrant, where his phone number was associated with a Google account.[105] They then sent Google another warrant specifically seeking data from Williams's account relevant to the crime.[106] Absent this first keyword warrant, the police would not have had this concrete information linking Williams to the scene and would not have found his concerning search history associated with crime.

Several keyword warrants have sought to identify everyone who searched for an address, but in other cases they have been used to search for variations of a victim's name or the name of someone related to the case.[107] In at least two cases, the queries have been broader. For example, an affidavit for a warrant filed in 2018 in connection to the serial Austin bombings, which resulted in the deaths of two people, asked the court to "require Google to disclose to the government copies of the information (including the content of communications)," and for information that satisfies a list of eight Boolean search terms, such as "("motion" OR "pull" OR "victim") AND ("bomb" OR "explosive" OR "explosion" OR "pipebomb" OR "pipe bomb" OR "PVC bomb")."[108] The request was made for "any IP addresses, User Agent Strings, and associated Google account information as further described . . . that entered the search terms"[109] belonging to those "who searched for the Google Search Terms between January 1, 2018 to March 2018," with no specific geographic bounds.[110] Further, the affidavit continued to suggest there was "probable cause" for the requested warrant.[111]

This request was made to Google because the company maintains records of IP addresses associated with the searches

---

Premises Controlled by Google, No. 1:18-mj-00191-ML (W.D. Tex. Mar. 19, 2018).

105. *Supra* notes 7–12 and accompanying text (detailing how police used the information obtained from keyword search warrants to link Williams's IP address to his phone number, and ultimately to link Williams to the arson).

106. *See* Ng, *supra* note 2.

107. Ray, *supra* note 1; *see also* Brewster, *supra* note 4.

108. Affidavit, *supra* note 104.

109. *Id.* at 8.

110. *Id.* at 3.

111. *Id.* As this warrant was leaked, there is little to no record of the judiciary's action in this case. Yet, the warrant is still a vital example of how these techniques are currently being used, and how advanced they have become: to find suspects for certain crimes and using a multitude of search terms.

conducted on its platforms. An IP address is assigned to an individual computer or cellphone and not the user's account, but it can be then used to find the owner of the device.[112] These addresses are often linked to account information accessed by the device, including email transaction information and application information used to "identify the account's user."[113] This may include the full name, physical address, telephone number, means and source of payment, and more information. The implications of such warrants are undefined, and it is unclear how many users had their information compromised in this case. Even more, it is unclear what the limits of such requests are absent legislation or litigation challenging their constitutionality.

Some of the top questions posed to Google are "how to register to vote," "how to get pregnant," "how to have sex," and "how to be happy alone."[114] As demonstrated, even a simple search for an address can be revealing; not only could this be used to find the location of a crime like arson, but knowing that a person searched for an address for Planned Parenthood could be incriminating.[115]

C. FROM IP TO THE INDIVIDUAL: HOW A KEYWORD WARRANT IS EXECUTED

The process of obtaining a reverse warrant can be undertaken in two or three steps. First, the government requests providers search their databases to produce an anonymized list of the IP addresses who have searched the listed terms.[116]

---

112. *See Privacy at Google*, GOOGLE 7 (2018), https://static.googleusercontent.com/media/services.google.com/en//blog_resources/google_privacy_booklet.pdf [https://perma.cc/DGR4-VZCA].

113. *Id.* at 4. A similar approach was used to link Williams to the R. Kelly case, as discussed in the Introduction, *supra*.

114. *See The Most Asked Questions on Google*, MONDOVO, https://www.mondovo.com/keywords/most-asked-questions-on-google [https://perma.cc/9MGN-RMWJ]; *Year in Search 2021*, GOOGLE, https://trends.google.com/trends/yis/2021/US [https://perma.cc/AHA8-EMUX].

115. Additionally, search engines may use "autocomplete" features that rely on algorithmic predictions of search queries based on a user's geographic location, past searches, language, and "common and trending queries." *See* Danny Sullivan, *How Google Autocomplete Predictions Are Generated*, GOOGLE (Oct. 8, 2020), https://blog.google/products/search/how-google-autocomplete-predictions-work [https://perma.cc/AZH6-R9WR]. This can lead to a user accidentally accepting a predicted search term, and thus entering queries they never intended.

116. *See, e.g.*, Affidavit in Support of an Application for a Search Warrant, *supra* note 8, at 7–8; Application for Search Warrant, No. 27-CR-CV-17-1 (Minn. Dist. Ct. Feb. 1, 2017), https://www.documentcloud.org/documents/3519211-

When a user makes a search, Google keeps a few key pieces of information: the search query (i.e., "how to make a bomb"), the time and date it was typed, the IP address and cookie of the computer it was entered from, and its browser type and operating system.[117] An IP address is assigned to an individual computer or cellphone and not the user's account, but it can then be used to find the owner of the device.[118] Additionally, once a user is logged in, Google automatically tracks the IP address that has recently utilized the account, for example, which IP addresses have recently accessed a Gmail inbox.[119]

After judicial approval, a warrant is then issued to a private company such as Google. At step one, an order is filed compelling disclosure of a de-identified list of all users whose accounts have searched the listed terms in a given time period.[120] Google does not know which users have this data prior to conducting this search and will have to search all of its data to identify users who searched the terms in a given timeframe.[121] For example, in the R. Kelly case, the judge authorized a warrant to Google for users who had searched the address of the residence close in time to the arson, which gave law enforcement a list consisting of IP addresses associated with times, dates, and locations that fell under the parameters of the warrant.[122] Sometimes, law enforcement will ask for personally identifying information at this stage, thus receiving the list of IP addresses at the same time they are receiving account information such as names, emails, and cellphone numbers.[123]

Edina-Police-Google-Search-Warrant-Redacted.html [https://perma.cc/PX5H-TYQ2].

117. *Privacy at Google*, *supra* note 112, at 6.

118. *Privacy at Google*, *supra* note 112; *see also* sources cited *supra* notes 105–07 and accompanying text (demonstrating how a keyword warrant can help the government identify the Google user who searched for a particular term).

119. Sophie Webster, *Google Account: How to Trace Other Devices Logged into Your Account*, TECH TIMES (Nov. 12, 2021), https://www.techtimes.com/articles/267901/20211112/google-account-trace-devices-logged.htm [https://perma.cc/H277-G4B8].

120. Google Amicus Brief, *supra* note 13, at 12–13.

121. *Id.*

122. *See, e.g.*, Affidavit in Support of an Application for a Search Warrant, *supra* note 8, at 7

123. *See, e.g.*, Application for Search Warrant, No. 27-CR-CV-17-1, *supra* note 116.

Second, law enforcement reviews the list and determines the users it is interested in investigating.[124] Sometimes, it will request additional information. If law enforcement has not yet received account identifying information, then they will ask the service provider for this information at this stage.[125] Finally, law enforcement may issue an individual-specific warrant for those identified.[126] These warrants may include searches of other devices the individual is linked to or physical spaces.[127]

III. THE HOLE IN THE DOCTRINE, OR HOW FOURTH AMENDMENT JURISPRUDENCE FAILS IN THE FACE OF TECHNOLOGY

This Note presumes that keyword search warrants are Fourth Amendment searches. Though admittedly an open question, both courts and Google have suggested that other reverse warrant techniques are Fourth Amendment searches,[128] and the Supreme Court has maintained that traditional warrants are generally preferred.[129] On the other hand, there is a strong argument that the third-party doctrine applies to these warrants, suggesting that data may be provided to law enforcement whether or not keyword search warrants are considered unconstitutional Fourth Amendment searches.[130] Thus, although an individual's expectation of privacy regarding their keyword

124. *See, e.g.*, Affidavit in Support of an Application for a Search Warrant, *supra* note 8, at 7–9 (asking the court for further information as a result of previously obtained IP addresses linked to Williams).

125. *Id.*

126. Hamilton, *supra* note 6; *see also* Google Amicus Brief, *supra* note 13, at 2–3, 14.

127. Google Amicus Brief, *supra* note 13 (discussing types of warrants based on the "Geofence").

128. *See, e.g.*, *In re* Search of Info. Stored at Premises Controlled by Google, 481 F.Supp.3d 730, 734 (N.D. Ill. 2020); Google Amicus Brief, *supra* note 13, at 4–5.

129. *See, e.g.*, Texas v. Brown, 460 U.S. 730, 735 (1983) (plurality opinion).

130. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("Whether the Government employs its own surveillance technology . . . or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements . . . ."); United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (discussing how electronic surveillance does not depend on a physical invasion of property and what that means for expectations of privacy); *see also* Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring) (expanding on the idea of what types of privacy are expected).

search (and related IP address data) may be considered reasonable, there exists a hole in constitutional protections: while a keyword search warrant is a Fourth Amendment search, the data sought is still likely protected under the third-party doctrine. Therefore, the data can still be reached without constitutional barrier, despite the reasonable interest an individual has in retaining this information as private. This Note aims to demonstrate the sizable hole in personal privacy protection that this current jurisprudence creates, in part due to the narrow defense available against the third-party doctrine.

Carpenter suggests that the third-party doctrine is not a bright line test, and guides courts to consider certain factors.[131] As the *Carpenter* Court recognizes, new technologies do not always "fit neatly under existing precedents."[132] Notably, the majority recognized "a world of difference between the limited types of personal information addressed in *Smith* and *Miller*, and the exhaustive chronicle of location information" at issue through CSLI collection.[133] While the resolution of specific technologies, like utilizing keyword search history, will be fact-dependent, these factors are still useful in analyzing how various technologies may be interpreted by the courts.

A. THE *CARPENTER* FACTORS OF REASONABLENESS

While *Carpenter* did not impose a bright line test, it did describe several factors relevant to its decision. There is disagreement about a precise list of *Carpenter* factors, and lower courts have emphasized various combinations.[134] Still, Chief Justice Roberts isolates three factors: (1) the deeply revealing nature of the information sought; (2) its depth, breadth, and comprehensive reach; and (3) the inescapable and automatic nature of its collection.[135] In many lower court opinions, it is important to

131. *See infra* Part III.A.

132. *Carpenter*, 138 S. Ct. at 2209; *see* Rachel Levinson-Waldman, *Cellphones, Law Enforcement, and the Right to Privacy*, BRENNAN CTR. FOR JUST. (Dec. 20, 2018), https://www.brennancenter.org/our-work/research-reports/cellphones-law-enforcement-and-right-privacy [https://perma.cc/HC3X-3QMG].

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

134. *See* Matthew Tokson, *The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018–2021*, 135 HARV. L. REV. 1790, 1822 (2022) (finding that courts cited a "variety of factors" in cases regarding *Carpenter* questions but rarely discussed all or most of the factors together, instead discussing factors that influenced their reasoning and ignoring others).

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

note that the number of persons affected by a surveillance practice was "rarely discussed and had virtually no effect on case outcomes"—several courts even rejected this factor given the limit of the *Carpenter* holding to the case at hand.[136]

As scholars suggest, "the widespread lower court adoption of *Carpenter* and the apparent administrability of its standards may bolster arguments for preserving and extending it, even as its future has become uncertain given recent changes in Supreme Court personnel."[137] There is a substantial possibility that future opinions will rely on *Carpenter*, and these factors will be used to identify the zone of reasonable protection.[138]

1. The Deeply Revealing Nature

First, the *Carpenter* opinion turned to the "deeply revealing" nature of the data: it was deeply revealing of some private quality of the person under surveillance.[139] To determine whether data is deeply revealing of the individual's privacies of life, analysis focuses on the nature of information rather than on the methods used to gather the information.[140] This suggests that the Court's analysis may apply to other massive collections of historical information such as browsing history. As understood by scholars, information stored by a private party thus must be sensitive or intimate to implicate a reasonable expectation of privacy test.[141] To be sensitive, information must be capable of being used to cause an individual or group harm; in contrast, intimate information reveals something important and not widely

136. *See generally* Tokson, *supra* note 134 (discussing concerns with the number of persons affected by surveillance practices and concerns with other potential factors in *Carpenter* analyses).

137. *Id.* at 1795. The author also concludes that there is a substantial possibility that future opinions will be fractured, with a pro-*Carpenter* plurality plus separate concurrences focusing on overtly textualist or originalist arguments. *Id.* at 1835.

138. *Id.* at 1794 (finding 857 citations of *Carpenter* from June 22, 2018 to March 31, 2021 in federal and state courts). Notably, only 34.1% of rulings applying *Carpenter* that did not end in a good faith exception found that there had been a Fourth Amendment search. *Id.* at 1809.

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

140. *Id.* at 2219 (citation omitted) (discussing how some cases did not rely solely on the methods, but rather the nature of the documents).

141. *See* Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1133–34 (2015); *see also* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 512–15 (2007) (discussing the private facts model).

known about a relationship between individuals.[142] The notion that detailed location information, implicated by analogous geofence warrants, can reveal one's "familial, political, professional, religious, and sexual associations," as Justice Sotomayor opined in her *Jones* concurrence, has been widely used as a representation for sensitivity of information.[143]

2. The Depth, Breadth, and Comprehensive Reach

Second, the *Carpenter* opinion considers information that possesses "depth, breadth, and comprehensive reach."[144] Like the first factor, inquiries into this factor focus on the intrinsic nature of the data at hand. Depth refers to the detail and precision of the information stored.[145] Breadth refers to how frequently the data is collected and how long the data has been recorded, adding gloss to the qualitative, intrinsic nature of the inquiry.[146] Comprehensive reach refers to the number of people tracked in the database.[147]

3. The Inescapable and Automatic Nature of Data Collection

In contrast with the preceding two factors, the inescapable and automatic nature of collection moves beyond intrinsic nature to discuss what has been done or could reasonably be done to protect data collection.[148] The third factor asks whether the target of surveillance assumed the risk, or if there is a reasonable

142. Ohm, *supra* note 141, at 1133–34 (focusing on how sensitive personal information is different from basic, personal information).

143. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

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

145. *Id.* at 2218 ("From the 127 days of location data it received, the Government could, in combination with other information, deduce a detailed log of Carpenter's movements, including when he was at the site of robberies. And the Government thought the CSLI accurate enough to highlight it during the closing argument of his trial.").

146. *Id.* at 2212 (highlighting the courts consideration of numerical standards as an indicator of the data's breadth by stating that "altogether the Government obtained 12,898 location points cataloging Carpenter's movements—an average of 101 data points per day").

147. *Id.* at 2218 ("Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may—in the Government's view—call upon the results of that surveillance without regard to the constraints of the Fourth Amendment. Only the few without cell phones could escape this tireless and absolute surveillance.").

148. *Id.* at 2219 (discussing reasonable expectations of privacy).

expectation of privacy relevant to the data's collection. Most directly linked to the third-party doctrine, it questions whether the subject knew that their information was exposed to the private party and willingly participated in such disclosure.[149]

These three factors comprise much of the key rationale behind *Carpenter*'s limitation of the third-party doctrine and can be helpful in assessing which other technologies should receive the same treatment.

If the keyword search technique is found to be violative of the Fourth Amendment for reasons of probable cause or particularity, which is an individual determination and outside the scope of this Note, then courts will consider whether or not to apply the third-party doctrine. In doing so, they likely will go through the *Carpenter* factors.[150] When used to analyze keyword search warrants, however, it becomes clear that the *Carpenter* decision's narrow ruling leaves many threats to personal privacy in limbo.[151] Keyword search warrant techniques are likely not going to receive the same treatment as CSLI data; yet they pose an equally significant threat.[152] They will remain in limbo, as will an individual's protection against them.

B. THE SHALLOW NATURE OF DE-IDENTIFIED IP ADDRESSES

In stage one of the keyword warrant process, law enforcement asks search engine providers to provide a list of IP addresses that have searched a given term in a given location during a certain time period.[153] These addresses are de-identified, and do not provide information on the individual who searched the terms to government officials. However, all of the IP addresses provided are confirmed to have searched the given term

149. This disclosure analysis is not without its limits. *See id*. at 2220 ("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.") (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979)).

150. *Id.* at 2223 (listing the factors).

151. *Id.* at 2220 (discussing the effect of a narrow ruling).

152. *See generally* Brewster, *supra* note 4 (addressing concerns of data privacy and keyword warrants).

153. *See* Affidavit in Support of an Application for a Search Warrant, *supra* note 8, at 7–8; Application for Search Warrant, No. 27-CR-CV-17-1, *supra* note 116 (discussing what law enforcement requested from Google, Inc.).

at the given time, in the given geographic location—hence, there is already some tracking availability.[154]

Most courts have found an IP address to fall under the umbrella of the third-party doctrine, and thus to not rise to the same level of revelation as CSLI data.[155] Notably, courts have found that "an internet user generates the IP address data that the government acquired . . . only by making the affirmative decision to access a website or application"; in contrast, CSLI data is generated when a cellphone receiving a message pings to the nearest cell tower regardless of user action.[156] This distinction between passive and active use has been a key contention in post-*Carpenter* litigation of IP address and account data—the type of data at issue in keyword search warrants.[157] However, it is arguably erroneous, as it fails to consider the societal necessity of using the internet, and thus the necessity inherent in generating IP address data.[158] This necessity and inescapability argument is central to the majority's reasoning in *Carpenter*, yet following decisions are unable to achieve this holistic purpose in favor of preserving the narrowness of the ruling.[159]

1. The Deeply Revealing Nature

The revelatory nature of the data in question is one of the most cited factors following *Carpenter*.[160] In cases with a determinative decision, courts almost never failed to find a search after determining that surveilled data was revealing, and never

154. *See* Affidavit, *supra* note 104 (providing examples where IP address information is used to provide geographic location of suspects, and how IP address information can be used in conjunction with keyword searches to provide precise location); *see also* Ray, *supra* note 1 (demonstrating another example of geofence warrants for user location data at specific times).

155. *See* Tokson, *supra* note 134, at 1829 ("Of the 217 cases that reached a determinative ruling on a Fourth Amendment search, 159 involved digital-age data such as IP addresses, cell site location data, or web-surfing data. Courts found a search in 57 of these cases, a rate of 35.8%.").

156. United States v. Hood, 920 F.3d 87, 92 (1st Cir. 2019).

157. *See generally* Tokson, *supra* note 134 (discussing the general aftermath of *Carpenter* in the courts).

158. *See infra* notes 192–94 and accompanying text.

159. *See* Tokson, *supra* note 134, at 1814 (demonstrating that judges take time to adjust to the post-*Carpenter* landscape).

160. Tokson, *supra* note 134, at 1823 ("The revealing nature of the data collected was mentioned in 93 total decisions [post-*Carptenter*].").

found a search after determining that surveilled data was unrevealing.[161] While many fact patterns involved CSLI data and thus were directly analogous to *Carpenter*, a handful of cases did discuss IP address information, finding it dissimilar in its revelatory nature. In *Heeger v. Facebook, Inc.*, for example, the Court found no constitutional violations related to Facebook's collection of IP addresses.[162] "The fact that the IP addresses at issue here are assigned to cell phones does not lead to a different conclusion . . . CSLI data is much more sticky and persistent" than IP address data, and the latter is less detailed.[163]

Likely, a list of unidentified IP addresses (that is, IP addresses that are not connected to account identifying personal information) that have searched a given term is not going to be considered to have the same "deeply revealing nature" that CSLI data has under *Carpenter*. It does not "provide an intimate window in a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations."[164] While this is a massive collection of historical information akin to that of CSLI data, it does not offer the same tracking ability that CSLI data does at this stage due to its unidentified nature.[165]

2. The Depth, Breadth and Comprehensive Reach

The second factor, while less determinative to the courts, may be more debatable. Depending on the key terms of the warrant, an individual may not have a reasonable expectation of privacy in their de-identified IP address under the depth, breadth, and comprehensiveness factor. Importantly, while the *Heeger* court found no reasonable expectation of privacy in IP address data, the *Heeger* decision considered IP address data associated with cell phone numbers and not keyword search terms; it is

161. *Id.* at 1823.

162. 509 F. Supp. 3d 1182, 1190–91 (N.D. Cal. 2020).

163. *Id.* at 1190 (finding that telephone subscribers know their numbers are used by telephone companies, and device users should "know that [IP address] information is provided to and used . . . for . . . directing the routing information").

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

165. *Compare id.* (demonstrating how identifiable CSCI data is), *with Heeger*, 509 F. Supp. 3d at 1189–90 (discussing the unique IP addresses that make identification challenging).

plausible that an IP address linked to the time, date, and term searched may reach a different conclusion.[166]

Depth may be understood as having the potential to betray a person's "familial, political, professional, religious, and sexual associations," if it is sufficiently precise.[167] Applied to this primary stage of a hypothetical warrant, the only information that law enforcement knows is that someone at a certain IP address searched for a given term at a given location and time.[168] Analysis must, then, turn on the words in question. If, for example, a warrant asked for those who searched "explosive", this would not have the same potential to reveal such intimate information. However, if a warrant asked for a list of those who searched "where to get an abortion," one could infer their politics, sexual history, religion, and sexual associations—a much more deeply revealing inquiry.[169]

Yet this stage still does not point to any personally identifying information, such as the individual's name or address, and thus law enforcement does not yet have the same paintable picture famously emphasized in *Carpenter*.[170] Further, courts have suggested that an IP address, absent any other information, does not allow the government to "effectively travel back in time": they are only forward-looking.[171] In comparison, CSLI records are collected by the provider and accessible retroactively to paint a picture of one's location.[172]

---

166. *Heeger*, 509 F. Supp. 3d at 1190 ("There is no legally protected privacy interest in *IP addresses alone*, which is the only interest plaintiffs concretely allege.") (emphasis added).

167. *Carpenter*, 128 S. Ct. at 2217 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)). *See generally supra* notes 144–47 and accompanying text (discussing depth, breadth, and comprehensive reach).

168. *See, e.g.*, Hamilton, *supra* note 6 (discussing how, at first, law enforcement only had associated IP addresses to their investigation).

169. This is already happening using Facebook messages: a Nebraskan woman was charged with multiple felonies for helping her teenage daughter get an abortion. Key evidence was found in their Facebook conversations, which showed her coaching her daughter on how to take the abortion pills. The warrant did not mention abortion at all, and Facebook maintains the handoff was valid and legal. Martin Kaste, *Nebraksa Cops Used Facebook Messages to Investigate an Alleged Illegal Abortion*, NPR (Aug. 12, 2022), https://www.npr.org/2022/08/12/1117092169/nebraska-cops-used-facebook-messages-to-investigate-an-alleged-illegal-abortion [https://perma.cc/7W7E-93B9].

170. *Carpenter*, 138 S. Ct. at 2213–18.

171. United States v. Soybel, 13 F.4th 584, 593 (7th Cir. 2021) (internal quotation marks omitted), *cert. denied*, 142 S. Ct. 835 (2022).

172. *See Carpenter*, 138 S. Ct. at 2212 (disclosing the facts that involved

While courts are correct in finding that IP address data does not alone provide this ability, historical keyword data is retroactive and provides this ability to retroactively paint a picture. The Seventh Circuit makes a notable distinction that IP information cannot show a glimpse into the mind of an individual: any intrusion on IP data cannot intercept the *content* of communications.[173] However, when combined with keyword information, this search technique begins to blur the line towards content interception.[174]

Despite this potentially blurred line, it is still likely that, given precedent, this first stage of a keyword search warrant will not be considered violative of the Fourth Amendment. As the Seventh Circuit has postulated post-*Carpenter*, "the unique features of historical CSLI are absent for IP-address data," notably that the IP address connection shows only that someone was using the internet, not who.[175] An argument could be made that this distinction could also plausibly be made for CSLI data in that it only shows the phone was present, and not that the owner was; anyone could plausibly have been in possession of the phone and still the ping would have occurred to the nearest tower.[176] Yet it is the whole picture that courts will analyze, and this whole picture may turn not on the IP address itself, but on the terms included in the search request.

This second factor (the depth, breadth, and comprehensive reach) may cause legal analysts to turn to the search terms in question, rather than the IP address itself, to determine depth of information. A single term or list of terms will admittedly not have the same revelation effects as seven days' worth of CSLI data. However, absent limits on the breadth of a keyword search warrant,[177] a longer list of terms may begin to reveal a greater

---

CSLI data being collected from the four-month period the robberies in question took place).

173. *Soybel*, 13 F.4th at 593 (emphasis added).

174. *Id.* (suggesting that the difference in the types of data, notably the content available, is key to the decision of whether or not *Carpenter* may be plausibly interpreted to include IP address data alone).

175. *Id.* at 592.

176. This is analogous to the argument used by the Florida biker, who was implicated in a burglary by a geofence warrant using data collected from his RunKeeper app, which placed him at the scene of a crime he was unaware had occurred. *See* Lyons, *supra* note 20.

177. Currently, these search warrants are up to individual judicial discretion and have no formal limits. There have been no court rulings placing limits

level of personal information. For example, connecting "where to get an abortion" to "abortions for minors in X state" to "abortions near X address" in a state where abortions are outlawed. This illustrates the current potential for police to string certain words together to catch anyone of a crime of their choosing—in this case, for an underage abortion in a state where abortions may be outlawed.[178]

It is when the keywords are added to the IP address information that the line begins to blur.[179] While simply searching "where to get an abortion" may not reveal as much, the combination of the three aforementioned terms begins to paint a picture of a minor looking for an abortion, cognizant of the illegality. In combination with the minor's IP address data, location, and the time the terms were searched, the police may begin to paint a similarly comprehensive picture at issue in *Carpenter*.[180] In the case of less detailed warrants, which have been common thus far, this comprehensive picture is not as likely.[181] Overall, "depth, breadth and comprehension" is more contestable when applied to IP addresses, especially when de-identified to the account, and may, in fact, depend on the individual user.[182] However, courts have already shown their reluctance to extend the

---

on these types of warrants, and cases have varied dependence on the judicial interpretation of the warrant.

178. *Supra* note 169 and accompanying text.

179. *Supra* notes 167–69 and accompanying text.

180. *See* Carpenter v. United States, 138 S. Ct. 2206, 2213–18 (2018) (painting the picture of the importance of gaining this data for law enforcement).

181. One way in which the court may analyze such information is the "mosaic theory" of the Fourth Amendment, by which courts evaluate a collective sequence of government activity as an aggregated whole to consider whether the sequence amounts to a search. Applying this to the consecutive revelation of IP addresses, keyword searches, and account information may provide a better analysis for keyword search warrant protocol. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).

182. The Federal Communications Commission (FCC) answered the precise question of whether web browsing records are private. The FCC enacted a privacy rule that the Trump administration quickly rolled back. *See* Brian Fung, *Trump Has Signed Repeal of the FCC Privacy Rules, Here's What Happens Next*, WASH. POST (Apr. 4, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/04/04/trump-has-signed-repeal-of-the-fcc-privacy-rules-heres-what-happens-next [https://perma.cc/ZLR4-9TCG]. In these proceedings, Internet Service Provider (ISP) supporters argued that their view into individual habits lacked depth and breadth because individuals may utilize multiple ISPs—their phone, home broadband connection, and work connection all utilize a different ISP, causing plausible distinguishability by the police. *See* Peter Swire, Justin

Carpenter doctrine to such data, and this will be a large hurdle to overcome.[183]

3. Inescapable and Automatic Collection

Inescapable and automatic collection of the data requested is again dependent upon the warrant in question. In *Carpenter*, the Court stated that "[c]ritcally, because location information is continually logged for all of the 400 million [cellular] devices in the United States . . . this newfound tracking capacity runs against everyone."[184] This is analogous to IP address data, as every user of the internet or of a search engine provider automatically generates this data, and it is retroactively accessible to law enforcement.[185] Additionally, every user of the internet generates search history and keyword data.[186] There are options which offer more privacy to the user. For example, DuckDuckGo pledges not to track a user's activity and keep it anonymous, but still retains the browsing history so that the individual user may return to a previously visited page; the search history still exists.[187] Other options like StartPage and Search Encrypt don't display terms in search history; if the user attempts to return to a page via the link, they will be returned to the search engine's homepage.[188] However, neither option is widely used. This factor would also depend on the detail of the keyword string asked for

---

Hemmings & Alana Kirkland, Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others 24–25 (Feb. 29, 2016) (unpublished manuscript), http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf [https://perma.cc/9UBP-86L3].

183. *See* Tokson, *supra* note 134, at 1832 (discussing general reluctance of courts to engage in extending *Carpenter*).

184. *Carpenter*, 138 S. Ct. at 2218 (noting the government's ability to surveil any cell phone user was not limited to "persons who might happened to come under investigation . . . [u]nlike with the GPS device . . . police need not even know in advance whether they want to follow a particular individual, or when").

185. *Id.*

186. *See* Tokson, *supra* note 134, at 1799 (discussing changes of the internet era regarding data disclosure of digital information).

187. Adam Benjamin, *DuckDuckGo: What to Know About the Privacy-Focused Search Engine*, CNET (Aug. 10, 2021), https://www.cnet.com/tech/services-and-software/google-search-rival-duckduckgo-what-to-know-about-the-private-search-engine [https://perma.cc/XY6V-DUWA].

188. *Id.*; *see also* Christian Stewart, *Is DuckDuckGo as Private as It Claims?*, MEDIUM (Mar. 5, 2019), https://medium.com/digiprivacy/is-duckduckgo-as-private-as-it-claims-5b4e30560b87 [https://perma.cc/GP8U-UD59] (comparing DuckDuckGo with Google and alternative privacy browsers in regard to search history records).

by the warrant. The more detailed string of abortion terms, analyzed in the above paragraph, would likely be considered more in-depth and to cover more breadth.

Likely, IP address data is automatic and inescapable, and keyword data is effectively so, despite the option to disable tracking. All internet traffic passes through internet service providers and is then linked to individual IP addresses which can record and are held by third parties accessible by the government under the third-party doctrine.[189] Courts have suggested that IP address data entails affirmative action (i.e., picking up the laptop or phone to conduct a search), and thus the data is not as automatically generated as CSLI data.[190] Further, Google maintains that a user's "profile" is only "[a]s specific as their use of Google['s] services."[191]

However, this argument fails to consider the societal necessity of using the internet. Like cellphones, the internet has become indispensable to participation in daily societal interaction.[192] While there are more options to escape keyword data than there are to escape IP address data, these options are not as widely utilized and may limit the usability of the internet.[193] Google dominates the search engine market worldwide at 92%, with Bing in second at 3.33% and DuckDuckGo in sixth at 0.71%.[194]

---

189. *See* Gabriel Weinberg, *Is It True That My ISP Is Spying on My Web Browsing? Does DuckDuckGo Fix That?*, QUORA, https://www.quora.com/Is-it-true-that-my-ISP-is-spying-on-my-web-browsing-Does-DuckDuckGo-fix-that/answer/Gabriel-Weinberg [https://perma.cc/9LCD-97U2]; Swire et al., *supra* note 182 (explaining the factual basis surrounding data collection by Internet service providers).

190. United States v. Soybel, 13 F.4th 584, 587, 593 (7th Cir. 2021).

191. *In re* Google Location History Litig., 514 F. Supp. 3d 1147, 1154 (N.D. Cal. 2021) (citation omitted).

192. United States v. Carpenter, 138 S. Ct. 2206, 2262 (2018) (Gorsuch, J., dissenting).

193. *See supra* notes 187–89 and accompanying text (discussing the more covert ways people might have to use the Internet to escape IP address data being used).

194. *Search Engine Market Share in 2022*, OBERLO, https://www.oberlo.com/statistics/search-engine-market-share#:~:text=DuckDuckGo%20wraps%20up%20the%20top,than%20one%2Dtenth%20of%20Google's [https://perma.cc/XRU3-NAGS]; *see also* Coral Murphy Marcos, *DuckDuckGo Search Engine Increased Its Traffic by 62% in 2020 as Users Seek Privacy*, USA TODAY (Jan. 18, 2021), https://www.usatoday.com/story/tech/2021/01/18/search-engine-duckduckgo-increases-traffic-google-competitor/4202556001 [https://perma.cc/8PVE-37LS].

While not as inescapable as CSLI data, which a user may not disable in any manner, ending the generation of keyword data is not easy and requires additional knowledge beyond the basic usage of browsers like Google. Further, misleading advertising of browsers who claim to be "private" but in reality still generate search history[195] make it so that browsing data remains a pervasive part of society.[196] Yet, it is that slight possibility that a user may choose not to generate keyword search history that courts will hold onto in applying *Carpenter*.

Courts have been reluctant to hold that IP address data alone satisfies the *Carpenter* factors, and therefore providing law enforcement with a de-identified IP address likely does not cause a Fourth Amendment search, even when combined with revelatory strings of keyword search terms.[197] Despite the indication that IP address data and keyword data combined may have the potential to combine to create inescapable, automatic, and comprehensive records, it is not as comparatively revealing of the individual as the CSLI data in *Carpenter*.[198]

This initial stage of a keyword warrant remains highly dependent on the terms at issue in the warrant, and there are currently no limitations. The nature of the information at this step is going to be the most likely barrier in suggesting a reasonable expectation of privacy in the unidentified information.

C. CROSSING THE LINE: ACCOUNT IDENTIFYING INFORMATION

At the second stage, law enforcement reviews the list of IP addresses and determines the users it is interested in. This is the step that courts have often considered as the "search" for

195. *See* Murphy Marcos, *supra* note 194 (demonstrating the extent that search engines track search history data).

196. *See* sources cited *supra* notes 187–91 and accompanying text (explaining how browsers marketed as private may still generate browsing history, and thus are potentially searchable by warrant). While there is technically a way to avoid leaving the trail, it is still not meaningfully voluntarily assumed as a risk; the user is not as aware of the data's collection as one may be in turning over bank records or phone records physically.

197. *See, e.g.*, United States v. Trader, 981 F.3d 961 (11th Cir. 2020); United States v. Soybel, 13 F.4th 584 (7th Cir. 2021).

198. Under the mosaic theory, this argument has a higher chance of success. However, there are still factual matters that are highly contested. *See* Kerr, *supra* note 181.

analogous geofence warrants.[199] As noted previously, law enforcement may either receive personally identifying account information in conjunction with IP information at the initial stage, or in a subsequent stage.[200] When this information is provided, it is far more likely but still not probable that courts will consider this to be of *Carpenter* nature, although this conclusion is not absolute.[201]

Unlike the first stage, the addition of account-linked information to a keyword search warrant may provide law enforcement with names (including subscriber names, user names, and screen names), addresses (including mailing addresses, residential, business, and email), phone records, records of session times and durations, temporarily assigned IP addresses, length of service, type of service, and identifying numbers of the device that was used to access search services.[202] This type of information has the potential to reveal the "familial, political, professional, religious, and sexual associations" that the Court has cautioned against,[203] such as in the case of the search query "where to get an abortion." Here, law enforcement agents can not only infer political, religious, and sexual associations, but they now have access to the individual's name, address, and telephone number and can match this information with a specific person.[204] This is especially true when considered under a mosaic theory analysis,

199. *See* Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2515–20 (2021) (finding that courts have implicitly treated the search as the point when the private company first provides law enforcement with the data requested as limited on the warrant application's face).

200. *Compare* Affidavit in Support of an Application for a Search Warrant, *supra* note 8, at 7–8 (requesting a warrant for both IP addresses and account information at the same time), *with* Application for Search Warrant, No. 27-CR-CV-17-1, *supra* note 116 (requesting account information after previously receiving IP address information).

201. *Supra* note 132 and accompanying text (finding that courts consider factors on a case-by-case basis, and the depth of information is one of the most weighty factors). *See generally* Tokson, *supra* 134.

202. Affidavit in Support of an Application for a Search Warrant, *supra* note 8, at 2; *see also* Application for Search Warrant, No. 27-CR-CV-17-1, *supra* note 116.

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

204. Application for Search Warrant, No. 27-CR-CV-17-1, *supra* note 116, at 6.

which suggests combining the effect of each step or piece of information to determine the effect that a search has on one's Fourth Amendment rights.[205]

1. The Deeply Revealing Nature

Alone, account identifying information has been considered as similar to business records and bank information, thus adequately falling under the third-party exception and searchable.[206] When connected to an IP address and a keyword, the account information only shows that an individual user searched a given word at a given location and time, and does not paint a comprehensive and detailed picture. Of course, when linked to multiple keyword searches, this inquiry becomes muddled.

If, like in the case of a search for the word "explosive," the information does not reveal such associations, it nevertheless allows law enforcement to track the individual user and determine not only their location but their inner thoughts at the presented time stamp. This is precisely the type of inquiry that *Carpenter* warned of. Notably, this inquiry does not cover an analog to the seven-day period at issue in *Carpenter*.[207] This single search is only one point of data. Nevertheless, it begins to show not only the location of an individual, but a look into their mind—an important distinction.[208]

Returning to the abortion example illustrates the potential detail in this second stage. Now, law enforcement would have account identifying information, such as the name or address of an individual, who searched "where to get an abortion", "abortions for minors in X state", "abortions near X address" in a state where abortions are outlawed, and may, in turn, discover more search terms this individual made. This is much more of a revealing nature and almost certainly not what the individual

205. Kerr, *supra* note 181; *see also supra* text accompanying note 198 (finding that courts consider factors on a case-by-case basis, and the depth of information is one of the most weighty factors).

206. *See, e.g.*, United States v. Caira, 833 F.3d 803, 805 (7th Cir. 2016) (considering subpoenas that may reveal the name, address, length of service, payment, IP information, and email of a suspect); United States v. Gregory, 2018 WL 7021080 (D. Neb. Oct. 29, 2018).

207. *Carpenter*, 138 S. Ct. at 2217 ("It is sufficient for our purposes today to hold that accessing seven days . . . constitutes a Fourth Amendment search.").

208. *Supra* note 156 and accompanying text (distinguishing between IP address data, showing an individual's internet searches, and CSLI data, showing a cell phone's location).

searching expected their data to be used for: the use is not objectively reasonable. In contrast, the pipebomb string of search terms,[209] when linked to the individual's name or address and IP address, while revealing, does not paint the same political or social values picture that Justice Sotomayor has warned of.[210] It is not as unreasonable or revealing, and thus again the inquiry returns to what list of terms would be deemed reasonable.[211] These three pipebomb-related searches would still likely not be enough to satisfy *Carpenter*, but begin to further blur the line.

A key contention the *Carpenter* court had with CSLI data is its ability to show location information, chronicling a user's location information simply from owning the device.[212] This is especially true when a user's account is linked to apps like Google Maps or Waze.[213] Unlike location information, the information that is collected via web and app activity does not continuously store information everywhere they go absent interaction.[214] However, courts have recognized that the detail of the collection and storage of such information is a factual question subject to further inquiry. It may be "collected and stored when no reasonable consumer would expect their location to be recorded," including for "non-location dependent internet searches such as 'chocolate chip cookies' on a Google device or Google browser."[215] As this may provide more geolocation-esque information, like addresses, there is a higher likelihood that courts will see analogues with CSLI data.

---

209. Affidavit, *supra* note 104; *see also supra* notes 107–10 and accompanying text.

210. *Supra* note 143 and accompanying text. This search does not include any information on the person's political or social leanings. Instead, it just points to criminal activity. While some may argue that abortion is a crime, this is a hotly contested social issue and not of the same nature as that of an illegal bombing.

211. This is a question of particularity and should be discussed further in subsequent academic literature.

212. *Supra* notes 82–88 and accompanying text. This information was only deemed as revealing because it was over seven days. Location information at a single time may be different, and thus the scope of the keyword information retrieved is critical to analysis. Indeed, *Carpenter* rests on long term surveillance to furnish its decision.

213. Affidavit, *supra* note 104 (suggesting that Google's services of Waze and Google Maps are of interest in the warrant process and may be connected with email accounts).

214. *In re* Google Location History Litig., 514 F.Supp.3d 1147, 1155 (N.D. Cal. 2021).

215. *Id.* at 1151.

Yet this is not without limitations. This factor remains highly dependent on the availability of account information connected to the IP address; in this case, the key dependency is the level of keyword search history available,[216] and how much detail the user provided when setting up their account.[217] Notably, courts tend to hyperfocus on the *amount of data* that is received during searches, and whether or not it is analogous to the seven-day *Carpenter* period. Additionally, the information provided is still limited to the list of search terms provided for in the warrant. Absent any meaningful restrictions on what can go into such a warrant, however, this remains a plausible Fourth Amendment search in certain circumstances.

2. The Depth, Breadth, and Comprehensive Reach

Second, the information provided by the provision of IP addresses connected to personally identifying account information may have potential to satisfy depth, breadth, and comprehensive reach. However, there remains sticky points that may suggest reluctance to find a reasonable expectation of privacy. In its analysis, the *Carpenter* Court turned to the "location data in combination with other information" that could "deduce a detailed log of Carpenter's movements" and highlighted the sheer number of data points: on average 101 per day.[218] An IP address linked with both the search term in question and information on a person's name, address, and screen time may paint a similar log of one's movements and activity, but only to a few key data points or times.[219]

While alone the IP address may not be as revealing, the combination of information is what is troubling. The IP address data provides law enforcement with information that can show the physical location of a user, and the warrant cabins this to show location, time and keyword searched. When combined with the

216. *Supra* notes 170–77 and accompanying text (describing how keyword searches may provide sufficient detail such that, when combined with IP addresses, the data falls into *Carpenter* territory).

217. *Supra* note 213 and accompanying text (showcasing that increased user detail, such as linked details between various Google apps, may provide a wider breadth of data, including location data).

218. Carpenter v. United States, 138 S. Ct. 2206, 2212, 2218 (2018).

219. *Supra* notes 203–05 and accompanying text (suggesting that a combination of CSLI data, IP address data, and keyword search terms could pose a larger Fourth Amendment threat).

account information, law enforcement may now know an individual's name, address, phone number, preferred browser, location at a given time through the IP address' tracking, and keyword terms. If a warrant is sufficiently broad enough in its time period or string of keyword terms, this may provide location, name, and thoughts of an individual before they are even linked to a crime. This becomes even more comprehensive when used to access an individual's entire browsing history, as done with Williams.[220] If linked to an IP address for a cellphone, this may provide a backdoor to accessing the very CSLI data at issue in *Carpenter*.[221]

Additionally, one may plausibly argue that data is comparatively comprehensive. As the Court critically includes, "because location information 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."[222] Analogously, Google alone has over one billion users of its products and services, with 60% of total Google searches coming from mobile devices.[223] Keyword search data is even more comprehensive: while Google does not share its volume data precisely, in 2020 there were 6.9 billion searches every day on Google alone; about 63,000 search queries every second.[224] However, such data is less broad than CSLI data: while CSLI data may be stored for up to five years, Google only stores its data for eighteen

220. *Supra* notes 12–18 and accompanying text (providing the procedure used to access Williams's personal devices and ultimately link him to his crime of arson).

221. *Supra* notes 12–18. Williams's IP address was ultimately linked to the keyword data, as has been the case in other keyword and IP address cases. *See, e.g.*, Heeger v. Facebook, Inc., 509 F. Supp. 3d 1182, 1189 (N.D. Cal. 2020) (illustrating the relation between IP addresses and CSLI data).

222. *Carpenter*, 138 S. Ct. at 2218. ("Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may—in the Government's view—call upon the results of that surveillance without regard to the constraints of the Fourth Amendment. Only the few without cell phones could escape this tireless and absolute surveillance.").

223. Ogi Djuraskovic, *Google Search Statistics and Facts 2022 (You Must Know)*, FIRST SITE GUIDE (Jan. 10, 2022), https://firstsiteguide.com/google-search-stats [https://perma.cc/JYU4-VMS9].

224. Christo Petrov, *The Stupendous World of Google Search Statistics*, TECHJURY BLOG (Apr. 1, 2022), https://techjury.net/blog/google-search-statistics [https://perma.cc/V7JP-KRNP]; *Number of Explicit Core Search Queries Powered by Search Engines in the United States as of October 2020*, STATISTA (Jan 18, 2021), https://www.statista.com/statistics/265796/us-search-engines-ranked-by-number-of-core-searches [https://perma.cc/RV67-NVKU].

months.[225] Despite this time limit, the depth and comprehensiveness of the data may likely overtake the lack of similar breadth, especially when investigating recent cases.

3. Inescapable and Automatic Collection

Third, while a user's IP address information is inescapably automatically collected, and collection of search history is difficult to get around,[226] this is not necessarily true of account identifying information. There are more capabilities for users to protect their account data than there are for CSLI and IP information, such as providing false names or emails, or not filling out the profile completely.[227]

However, it is still true to say that the use of technologies requiring the creation of a personal account are a "pervasive and insistent part of daily life", such as email and log-ins to various websites, and are thus not in a true sense "voluntary and escapable" as they relate to acting as a functioning member of today's society.[228] Although one could argue an individual user could turn on Google's incognito mode, or use more protective search engines like DuckDuckGo, all internet traffic still passes through ISPs, which can record browsing histories and are thus held by third parties accessible by the government under the third-party doctrine.[229]

Like cellphones, the internet has become indispensable to participation in daily societal interaction.[230] In fact, the internet is frequently accessed on a cellphone, creating mobility and

225. *Carpenter*, 138 S.Ct. at 2218; *see also* Lily Hay Newman, *Limit How Long Google Keeps Your Data with This Overdue Setting*, WIRED (May 7, 2019), https://www.wired.com/story/google-auto-delete-data-privacy-setting [https://perma.cc/96F8-28YL].

226. *Supra* notes 179–87 and accompanying text (showing that it is difficult for users to avoid having search engines track their search history, which, in combination with IP address and CSLI data, poses a Fourth Amendment threat).

227. *See* Weinberg, *supra* note 189 (detailing the privacy risks of web browsing).

228. *Carpenter*, 138 S. Ct. at 2220 (quoting Riley v. California, 134 S. Ct. 2473, 2484 (2014)); *id.* at 2220 ("[A] cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI . . ."). This lack of affirmative act is also found in the production of account information, but one *may* take some level of affirmative action to stop the collection of data or attempt to mask the data.

229. Weinberg, *supra* note 189.

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

search capabilities at one's fingertips. Given the Supreme Court's past concessions that such technologies are a prerequisite to modern societal participation,[231] and that collection of such data is inherent in the use of search-related services, it is likely that courts will see keyword search data as satisfying this third factor when combined with other data as accessed by search warrants, given limitations on the terms at issue.[232]

It is for these reasons that this second step of the keyword warrant process is more likely to hold a reasonable expectation of privacy, but this is still not probable in many cases. Courts should require adequate showing of probable cause and particularity before providing account identifying information. Although there remains uncertainty, the revealing nature of the information accessed is the ultimate test of *Carpenter*. If a warrant is found to be violative of the Fourth Amendment, then Courts will likely go through a similar analysis to the above. As the factors showcase, keyword warrants will likely not receive *Carpenter* extended protection. Thus, a sizeable gap in protection exists: if a keyword warrant is considered a proper Fourth Amendment search, then one's data is accessible. If a keyword warrant is not considered a proper Fourth Amendment search, the information will likely be accessible through the third-party doctrine. Thus, a legislative solution is needed.

IV. CLOSING THE GAP: A PUSH FOR LEGISLATIVE ACTION

Keyword warrants are facing their first direct challenge in court in *People v. Seymour*, with a group of teenagers charged

231. *Id.*

232. While not an official step of the keyword warrant process, many keyword warrants lead law enforcement to file additional warrants to obtain an individual's information through CSLI data. In the R. Kelly case, for example, law enforcement linked two IP addresses to a telephone number belonging to Williams, and then used this to investigate location information associated with the individual's telephone number. Additionally, police also combined the telephone information with email information to create a detailed picture of the defendant's steps. *See* Affidavit in Support of an Application for a Search Warrant, *supra* note 8, at 7–9. This step is the most analogous to *Carpenter*, as it is exactly the kind of data the Court analyzed, and the kind of data most likely to be found a search in subsequent *Carpenter* caselaw. *See* Tokson, *supra* note 134, at 32 (finding that the data method was a factor in the application of *Carpenter* in lower courts). It also illustrates the potential for such techniques to be used as a backdoor method to access information, and the potential to exploit citizen usage of personal technologies.

with residential arson that killed a family of five.[233] The teenagers were identified by Google search requests for the address at which the arson took place, similar to the R. Kelly case.[234] Lawyers have filed a motion to suppress, arguing that this is a violation of the Fourth Amendment protection against unreasonable searches, analogous to general search warrants.[235] If this motion is successful, it would suggest that keyword search warrants may be violative of the Fourth Amendment. However, the question remains whether or not the third-party doctrine would apply, and thus whether *Carpenter* should be extended.[236]

Carpenter directs courts to limit the application of the third-party doctrine and find that, in some cases, there is a need for protection of the Fourth Amendment to be applied to online data. Based upon its opinion, *Carpenter* has the potential to become a canonical case: it represents a potentially fundamental shift of

---

233. Motion to Suppress Evidence from a Keyword Warrant & Request for a Veracity Hearing, People v. Seymour, No. 21CR20001 (D. Colo. 2022) [hereinafter Motion to Suppress], https://www.documentcloud.org/documents/22076537-motion-to-suppress-google-evidence-in-colorado-vs-seymour [https://perma.cc/4UVL-CG7D].

234. *Id.*; *see, e.g.*, *supra* notes 1–4 and accompanying text.

235. Motion to Suppress, *supra* note 233, at 2 ("No court has considered the legality of a reverse keyword search, but its constitutional defects are readily apparent and should have been obvious to all involved. It is a 21st century version of the general warrants that the Fourth Amendment was designed to guard against. Just as no warrant could authorize the search of every home in America, no warrant can compel a search of everyone's Google queries.").

236. The Motion to Suppress acknowledges this next step and argues that the "so-called 'third-party doctrine' is inapplicable." *Id.*

> Search queries are fundamentally different from the business records to which the third-party doctrine traditionally applies. *See Smith v. Maryland*, 442 U.S. 735 (1979) (numbers dialed on a landline); *United States v. Miller*, 425 U.S. 435 (1976) (bank deposit slips). Instead, they reveal information that is even more private than the seven days of cell phone location data that the Supreme Court found were constitutionally protected. *Carpenter*, 138 S. Ct. at 2206. Moreover, Google is no ordinary third party: 'Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible.' *Id.* at 2219. Indeed, records of Google search queries are comprehensive and inescapable, captured with every query, from every user, regardless of whether they are signed in to a Google account . . . . And because each query is tied to a unique ID number as well as the Internet Protocol ("IP") address assigned to each user, they are personally identifiable.

Motion to Suppress, *supra* note 233, at 2–3.

third-party doctrine, and the way we think about personal privacy. The Court has recognized that intrusive technologies should trigger higher judicial scrutiny.[237]

However, *Carpenter* leaves enough ambiguity about the continued role of the third-party doctrine that courts endorsing a strong third-party doctrine, such as one expanded to cover keyword search warrant techniques, are not overtly resisting *Carpenter*.[238] Yet, the likely outcome is that courts will choose to further restrict the application of *Carpenter*: the analysis above suggests that *Carpenter* will not apply to keyword techniques at either stage.

Thus, despite the potential illustrated for new investigative techniques to exploit personal privacies, it is likely that the Fourth Amendment and the third-party doctrine together create a lapse in protection, leaving individuals vulnerable. Courts will continue to use the third-party doctrine to draw a line between the CSLI data at issue in *Carpenter* and emerging technologies, remaining incredibly cautious to extend *Carpenter*-esque protections. Instead, some legislatures and liberties advocates have turned to legislative solutions.

Importantly, these emerging techniques access personally identifying account information and showcase that existing protection is not enough to protect against privacy intrusions in the digital age. While it may not be found to be the same as CSLI data in *Carpenter*, it provides a different *kind* of privacy risk: it begins to reveal the *content* of one's communications rather than simply location alone. Further, keyword searches and internet use are equally as integral to our modern society. Widespread lower court adoption of *Carpenter*[239] and the apparent administrability of its standard suggest that its holding will continue

237. *See supra* Part I (discussing the bounds of the Fourth Amendment when applied by the Court to technological advancements).

238. *See Carpenter*, 138 S. Ct. at 2220 (emphasizing the factually narrow nature of the decision and declining to overrule previous third-party doctrine cases).

239. Yet, these lower court opinions have been exceedingly reluctant to extend protections to third-party data sources other than CSLI data. *See, e.g.*, *In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 611–12 (5th Cir. 2013) (finding cell phone location data to be a business record that the government can access without a warrant); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (finding no Fourth Amendment protection for email or IP addresses). *But see* Ferguson v. City of Charleston, 532 U.S. 67, 84–85 (2001) (declining to allow the government to obtain data disclosed to state

to shape Fourth Amendment jurisprudence, but that *Carpenter* alone is not enough.[240]

Tech giants such as Google, Yahoo, and Microsoft have spoken out in favor of banning reverse search warrant techniques, like geofence and reverse keyword warrants, advocating for the passage of a bill before the New York State legislature.[241] The Reverse Location Search Prohibition Act would prohibit "the search, with or without a warrant, of geolocation and keyword data of a group of people who are under no individual suspicion of having committed a crime, but rather are defined by having been at a given location at a given time"[242] and includes any court order, "including a search warrant."[243] If passed, it would be the first state law to ban law enforcement from demanding tech companies turn over user data in these instances.[244]

Indeed, bills such as the Reverse Location Search Prohibition Act follow a growing trend for increased privacy litigation. Texas Attorney General Ken Paxton has filed a lawsuit against Meta for violating State law by capturing biometric identifiers without users' consent.[245] On a federal level, TechNet, one of the oldest tech interest groups, has met with forty-one lawmakers to address collection and use of user data and advocate for a federal privacy standard.[246] Post *Roe v. Wade*'s overrule, these requests

---

hospital employees, albeit in a case where the third-party doctrine issue was not expressly before the Court).

240. Tokson, *supra* note 134, at 4.

241. Zack Whittaker, *A Bill to Ban Geofence and Keyword Search Warrants in New York Gains Traction*, TECH CRUNCH (Jan. 13, 2022), https://techcrunch.com/2022/01/13/new-york-geofence-keyword-search-warrants-bill [https://perma.cc/RZF9-BZUB].

242. Reverse Location Search Prohibition Act, Assemb. B. 84A, 2021 State Assemb., Reg. Sess. (N.Y. 2021), https://legislation.nysenate.gov/pdf/bills/2021/A84 [https://perma.cc/KY2Y-TPT6].

243. *Id.*

244. Whittaker, *supra* note 241.

245. Christine Schiffner, *"The Tide Is Turning" on Big Tech as Plaintiffs Firms File More Data Privacy Lawsuits*, NAT'L L. J. (Feb. 16, 2022), https://www.law.com/nationallawjournal/2022/02/16/the-tide-is-turning-on-big-tech-as-plaintiffs-firms-file-more-data-privacy-lawsuits [https://perma.cc/JJV4-6GVW].

246. Brody Ford, *Big Tech to Congress: Forget About Antitrust, Pass a Privacy Law*, BLOOMBERG NEWS (Apr. 8, 2022), https://www.bloomberg.com/news/articles/2022-04-08/big-tech-to-congress-forget-about-antitrust-pass-a-privacy-law [https://perma.cc/VW9E-PUNF].

and discussion surrounding larger legislation has grown exponentially.[247] Privacy advocates have expressed renewed concerns about how tech platforms handle requests for data.[248] Tech platforms hold "vast troves of personal and health information in the form of the products we shop for, the places we travel, the businesses we frequent, the websites we visit, the information we search for, and the messages we send to our friends and family."[249] *Roe* and abortion has served as a catalyst for the conversation as digital rights groups warn of the risk this footprint may pose for abortion seekers.

Technology will only continue to evolve, and courts and legislatures alike must adapt their principles to the times. "A person does not," and should not be expected to, "surrender all Fourth Amendment protection by venturing into the public sphere."[250]

CONCLUSION

Historically, "the greatest protections of privacy were neither constitutional nor statutory, but practical."[251] Modern technology has removed many practical barriers to surveillance, causing our law to shift its focus to a new standard. Keyword search warrants further erode societal barriers, allowing law enforcement to outsource its investigative work and take advantage of our society's technological reliance. This is especially true when such investigative techniques are not limited by the type of inquiry they can make or any meaningful time period.

While the Supreme Court has taken important initial steps towards protecting our digital privacies, the rapidly evolving technologies inevitably leave gaps in protection. By cabining the analysis in *Carpenter* to the facts of the case, current judicial interpretations leave gaps in protections that the founders could not have considered. Scholars have written numerous articles addressing the problematic application of Fourth Amendment jurisprudence to a modern society, yet the judiciary is slow in its response. It is for this reason that legislative action should be

247. Brian Fung & Claire Duffy, *A Big Question for Tech Companies Post-Roe: How to Respond to Law Enforcement Requests for Data?*, CNN BUS. (June 28, 2022), https://www.cnn.com/2022/06/28/tech/big-tech-abortion-data-law-enforcement/index.html [https://perma.cc/T2NW-7N9M].

248. *Id.*

249. *Id.*

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

251. United States v. Jones, 565 U.S. 400, 429 (2012) (Alito, J., concurring).

considered, as it has the potential to create more nuanced solutions and continue the spirit of the Fourth Amendment, and the spirit of *Carpenter*.