WRONG SEARCH AT THE WRONG TIME: KEYWORD SEARCH WARRANTS AND THE FOURTH AMENDMENT

Nicole Chan†

TABLE OF CONTENTS

† Associate Editor, *Cardozo Law Review* (Vol. 45); J.D. Candidate, Benjamin N. Cardozo School of Law (June 2024); B.A., Stony Brook University (Dec. 2019). I would like to thank my family and friends for their unconditional love and support, Professor Gaia Bernstein for her feedback and guidance, and my colleagues on *Cardozo Law Review* for preparing this Note for publication.

INTRODUCTION

On August 5, 2020, five members of a family were killed when their house was set ablaze.[1] Kevin Bui admitted to investigators that he and two other teens burned the house down after his iPhone had been stolen.[2] He used the Find My application and located his phone at the Green Valley Ranch home.[3] It was not until the next day while reading the news about the arson that he realized he had targeted the wrong residence.[4]

The Denver Police Department was able to identify Bui and his accomplices by serving Google a keyword search warrant.[5] A keyword search warrant is a type of reverse search warrant that demands data about any and all individuals who have searched for certain keywords during a specified time period.[6] A reverse search warrant is significantly different from a traditional search warrant because the former is used by

---

1 Jon Schuppe, *Police Sweep Google Searches to Find Suspects. The Tactic Is Facing Its First Legal Challenge*, NBC NEWS (June 30, 2022, 2:27 PM), https://www.nbcnews.com/news/us-news/police-google-reverse-keyword-searches-rcna35749 [https://perma.cc/Z8GF-G7F4].

2 Elise Schmelzer, *Teen Charged in Deadly Denver Arson Told Investigators He Set Fire over Stolen Phone, Detective Says*, DENV. POST (Nov. 12, 2021, 6:05 PM), https://www.denverpost.com/2021/11/12/denver-green-valley-ranch-arson-homicide-hearing [https://perma.cc/4DXM-76HX].

3 *Id.*

4 *Id.*

5 Thomas Brewster, *Warrants Can Force Google to Look Through Your Search History—a Tragic Arson Case May Decide If That's Constitutional*, FORBES (June 30, 2022, 2:00 PM) [hereinafter Brewster, *Warrants Can Force Google*], https://www.forbes.com/sites/thomasbrewster/2022/06/30/warrants-can-force-google-to-look-through-your-search-historya-tragic-arson-case-may-decide-if-thats-constitutional/?sh=29533b8a6608 [https://perma.cc/33S3-KKBF].

6 Leslie Corbly, *Geofences Aren't the Only Reverse Warrants*, LIBERTAS INST. (July 1, 2022), https://libertas.org/justice-and-due-process/geofences-arent-the-only-reverse-warrants [https://perma.cc/7YHT-SAW8]; Matthew Guariglia, *Geofence Warrants and Reverse Keyword Warrants Are So Invasive, Even Big Tech Wants to Ban Them*, ELEC. FRONTIER FOUND. (May 13, 2022), https://www.eff.org/deeplinks/2022/05/geofence-warrants-and-reverse-keyword-warrants-are-so-invasive-even-big-tech-wants [https://perma.cc/Z8JC-3R75]; Notice of Declaration of Legal Investigations Support Analyst Nikki Adeli (Google Declaration) ¶ 11, People v. Seymour, No. 21CR20001 (Colo. Dist. Ct. June 30, 2022) [hereinafter Declaration of Legal Investigations Support Analyst], https://www.nacdl.org/getattachment/13d9ccb1-5e6d-4dfd-a8e2-57c32fafbc2d/google-declaration-of-nikki-adeli.pdf [https://perma.cc/5B4L-DP9Q].

law enforcement officials to find suspects to investigate.[7] A traditional search warrant, in contrast, is used by law enforcement officials when they have probable cause to believe that a specific individual has committed a particular crime.[8] The police in this case were unable to identify the perpetrators until they used a keyword search warrant.[9] Indeed, they had executed twenty-three other warrants prior to the keyword search warrant—to no avail.[10] The keyword search warrant was issued to Google and sought data on anyone who searched for nine variations of the address of the home prior to the fire.[11] Google executed a text-based query,[12] which returned sixty-one searches that were associated with five Google identifiers (GAIA IDs)[13] and three Browser Cookie IDs.[14] The warrant did not authorize additional information about those users to be disclosed, so the law enforcement officials served

---

7 *See* Schuppe, *supra* note 1.

8 *Search Warrant*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/search_warrant [https://perma.cc/9255-Q6TP] (May 2022); *see* Johana Bhuiyan, *The New Warrant: How US Police Mine Google for Your Location and Search History*, THE GUARDIAN (Sept. 16, 2021, 6:00 AM), https://www.theguardian.com/us-news/2021/sep/16/geofence-warrants-reverse-search-warrants-police-google [https://perma.cc/8CMC-ZWN5].

9 Motion to Suppress Evidence from a Keyword Warrant & Request for a Veracity Hearing ¶ 2, People v. Seymour, No. 21CR20001 (Colo. Dist. Ct. June 30, 2022) [hereinafter Motion to Suppress], https://www.nacdl.org/getattachment/6e9a8307-b22e-4c4d-a30b-e43aa6fe5d72/2022-06-30-11-50-04-220630-Seymour-MTS-FINAL-67.pdf [https://perma.cc/GU72-ENPU].

10 *Id.* ¶¶ 9–10.

11 The warrant requested information about Google users who had searched for the following terms: "5312 Truckee," "5312 Truckee St," "5312 Truckee Street," "5312 N Truckee St," "5312 N. Truckee St.," "5312 N. Truckee St," "5312 N Truckee St.," "5312 North Truckee," and "5312 North Truckee Street." Declaration of Legal Investigations Support Analyst, *supra* note 6, ¶ 13; Schuppe, *supra* note 1.

12 A text-based query allows Google to find all instances of a particular keyword in its records. *See* Shalin Hai-Jew, *Using NVivo: An Unofficial and Unauthorized Primer*, SCALAR, https://scalar.usc.edu/works/using-nvivo-an-unofficial-and-unauthorized-primer/text-search-query [https://perma.cc/TU7H-K22L] (Oct. 4, 2022).

13 *Access Control*, GOOGLE ISSUE TRACKER, https://developers.google.com/issue-tracker/concepts/access-control [https://perma.cc/679Q-LNMD] ("Gaia is the ID management system for all Google products. This ID may be an e-mail address associated with a Google domain (for example, user@gmail.com) or an e-mail address in another domain that has been configured by a Google Workspace domain administrator.").

14 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, 10:33 AM) [hereinafter Brewster, *Exclusive*], https://www.forbes.com/sites/thomasbrewster/2021/10/04/google-keyword-warrants-give-us-government-data-on-search-users/?sh=6aeacfc17c97 [https://perma.cc/QJL7-37MC] ("CookieIDs 'are identifiers that are used to group together all searches conducted from a given machine, for a certain time period. Such information allows investigators to ascertain, even when the user is not logged into a Google account, whether the same individual may have conducted multiple pertinent searches' . . . ." (quoting a sealed keyword search warrant that was issued by federal investigators in Wisconsin and reviewed by *Forbes*)); Declaration of Legal Investigations Support Analyst, *supra* note 6, ¶ 14.

Google with another warrant; the subsequent warrant requested identifying information associated with the five GAIA IDs.[15] Google produced the basic subscriber information for those users, which led investigators to find that the three teenagers had searched for the address multiple times in the two weeks before the fire.[16]

The lawyers for Gavin Seymour, one of the teens, are arguing that the search violated the Fourth Amendment's protection against unreasonable searches.[17] This case, *People v. Seymour*, is the first known case in the United States to challenge the constitutionality of keyword search warrants.[18] On November 16, 2022, Denver District Court Judge Martin Egelhoff upheld the constitutionality of the keyword search warrant and denied the defendant's motion to suppress evidence.[19] Judge Egelhoff found that the police acted appropriately and that the warrant was sufficiently narrow and supported by probable cause.[20] He rejected the argument that a violation of privacy had occurred and stated that the search was not overbroad because it was targeted.[21] The Colorado Supreme Court will review the ruling on the constitutionality of the keyword search warrant in the latter half of 2023.[22]

This Note will advocate for the view that when presented with the issue, state and federal courts should establish that keyword search warrants are unconstitutional because they violate the Fourth Amendment. Keyword search warrants cannot meet the Fourth Amendment's requirements of probable cause and particularity because the subjects of the search cannot be identified until after the search is

---

15 Declaration of Legal Investigations Support Analyst, *supra* note 6, ¶ 16.

16 *Id.*; Schuppe, *supra* note 1.

17 Schuppe, *supra* note 1.

18 Motion to Suppress, *supra* note 9; Jennifer Lynch & Andrew Crocker, *Update: Colorado Supreme Court Grants Review in First U.S. Case Challenging Dragnet Keyword Warrant*, ELEC. FRONTIER FOUND. (Jan. 18, 2023), https://www.eff.org/deeplinks/2022/06/eff-file-amicus-brief-first-us-case-challenging-dragnet-keyword-warrant [https://perma.cc/3BLA-M4PH].

19 Shelly Bradbury, *Green Valley Ranch Arson Suspects Signal They May Take Plea Deals After Judge Upholds Google Keyword Warrant*, DENV. POST (Nov. 16, 2022, 5:48 PM), https://www.denverpost.com/2022/11/16/green-valley-ranch-arson-diol-google-bui-seymour [https://archive.md/xLaCw].

20 *Id.*

21 *Id.* ("I liken this search to looking for a needle in a haystack, . . . [a]nd the fact that the haystack may be big, the fact the haystack may have a lot of information in it, doesn't mean a targeted search in that haystack somehow implicates overbreadth.").

22 *See* Jessica Seaman, *Colorado Supreme Court to Review Denver Police's Use of "Digital Dragnet" in Deadly Green Valley Ranch Arson Case*, DENV. POST (Jan. 20, 2023, 5:17 PM), https://www.denverpost.com/2023/01/20/denver-police-reverse-keyword-search-colorado-supreme-court [https://perma.cc/2XCG-R83L]; Lynch & Crocker, *supra* note 18.

completed.[23] These warrants are unnecessary and have the potential of implicating millions of internet users who have no connection to a crime.[24] This Note will contend that individuals have a reasonable expectation of privacy in their search history data, and that law enforcement officials violate the Fourth Amendment's protection against unreasonable searches when they obtain such data without a traditional search warrant.

Part I of this Note will provide the history, jurisprudence, and other background information necessary to this issue. To begin, Section I.A will present an overview of the Fourth Amendment by describing its history and role in protecting individuals against unreasonable searches and seizures. Next, Section I.B will describe what action is required for courts to find that a Fourth Amendment search has occurred. Subsequently, Section I.C will examine the third-party doctrine to illustrate circumstances in which individuals do not have a reasonable expectation of privacy. Then, Section I.D will examine the Supreme Court's decision in *Ybarra v. Illinois* to explain that probable cause must be particularized to every individual being searched. Section I.E will first examine the decision in *Carpenter v. United States* and then discuss the multi-factor test that emerged from the case. After, Section I.F will describe the various instances in which keyword search warrants have been used in the United States. Section I.G will discuss Google's procedures after it is served with a keyword search warrant. This Note focuses on Google because it is the most popular search engine and has disclosed its procedures in responding to keyword search warrants.[25] Part I will end with Section I.H, which will examine the decision in *United States v. Chatrie* to show that similar warrants have been found to violate the Fourth Amendment.

---

23 U.S. CONST. amend. IV; Declaration of Legal Investigations Support Analyst, *supra* note 6, ¶ 5 ("Before running this query, Google and its records custodians do not know which, if any, users may have undertaken searches that would be responsive to the warrant in question."); Naomi Gilens, Jennifer Lynch & Veridiana Alimonti, *Google Fights Dragnet Warrant for Users' Search Histories Overseas While Continuing to Give Data to Police in the U.S.*, ELEC. FRONTIER FOUND. (Apr. 5, 2022), https://www.eff.org/deeplinks/2022/04/google-fights-dragnet-warrant-users-search-histories-overseas-while-continuing [https://perma.cc/28NQ-MH2K].

24 *See* Albert Fox Cahn & Amanda Humell, *'Keyword Warrants' Make Every Search a Risk*, VERFASSUNGSBLOG (Oct. 15, 2020), https://verfassungsblog.de/keyword-warrants [https://perma.cc/3E9W-59HM].

25 Google comprises about ninety percent of all web, mobile, and in-app searches, and data shows that 8.5 billion Google searches are conducted per day. James Eagle, *Animation: The Most Popular Websites by Web Traffic (1993–2022)*, VISUAL CAPITALIST (Sept. 9, 2022), https://www.visualcapitalist.com/cp/most-popular-websites-by-web-traffic [https://perma.cc/B8YS-2PK8]; Maryam Mohsin, *10 Google Search Statistics You Need to Know in 2022 [Infographic]*, OBERLO (Jan. 2, 2022), https://www.oberlo.com/blog/google-search-statistics [https://perma.cc/5KNK-BFE4]; Declaration of Legal Investigations Support Analyst, *supra* note 6, ¶¶ 2–10.

Part II of this Note will analyze keyword search warrants in the context of the Fourth Amendment to argue that keyword search warrants cannot be substituted for traditional search warrants. First, Section II.A will apply the *Carpenter* test to search history data to demonstrate that individuals have a reasonable expectation of privacy in their data, so a traditional search warrant is required to obtain such information. Following that, Section II.B will assert that keyword search warrants can never be based on probable cause, discussing the Austin serial bombings investigation to illustrate the point. Next, Section II.C will argue that keyword search warrants are unconstitutional because they do not meet the Fourth Amendment's particularity requirement. Then, Section II.D will argue that courts should hold keyword search warrants to be unconstitutional as they have for geofence warrants. Finally, Section II.E will explain that keyword search warrants are unnecessary because law enforcement officials can use less intrusive traditional investigative techniques to find perpetrators.

I. BACKGROUND

A. *The Fourth Amendment's History and Purpose*

The Fourth Amendment to the United States Constitution guarantees that individuals have a right to be free from "unreasonable searches and seizures" by the government.[26] The Founders wrote the Fourth Amendment as a response to writs of assistance that were used during the colonial era.[27] Writs of assistance were general search warrants, which were overbroad and unlimited in scope.[28] British officers were allowed to enter homes without any notice or reason and to search for evidence of criminal activity.[29] In a famous English case, *Entick v. Carrington*, the plaintiff challenged one of these general warrants, and the court held that the warrant was unlawful because it was not supported by probable cause.[30] The case was influential in the drafting of the Fourth

---

26 U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

27 Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (citing Riley v. California, 573 U.S. 373, 403 (2014)).

28 *See* Stanford v. Texas, 379 U.S. 476, 481 (1965).

29 *Carpenter*, 138 S. Ct. at 2213 (citing *Riley*, 573 U.S. at 403).

30 (1765) 95 Eng. Rep. 807, 817 (K.B.) ("[O]ur law holds the property of every man so sacred, that no man can set his foot upon his neighbour's close without his leave; if he does he is a trespasser, though he does no damage at all; if he will tread upon his neighbour's ground, he must justify it by

Amendment, and the United States Supreme Court has revered it as "the true and ultimate expression of constitutional law."[31]

Pursuant to the Fourth Amendment, a search warrant requires probable cause and particularity.[32] Probable cause exists when there is a reasonable basis for believing that evidence of a crime will be found in the place to be searched.[33] The particularity requirement is satisfied when the warrant has a specific description of the place to be searched and the items or people to be seized.[34] The requirement limits officers' discretion when executing a warrant.[35] A search warrant cannot be issued if the area it covers is too broad or if it does not identify specific people or items.[36] The Fourth Amendment only safeguards against unreasonable searches and seizures, and the test for whether a search is reasonable was established in *Katz v. United States*.[37]

---

law."); *History and Scope of the Amendment*, JUSTIA, https://law.justia.com/constitution/us/amendment-04/01-search-and-seizure.html [https://perma.cc/FUQ7-S7DS] ("Besides its general character, the court said, the warrant was bad because it was not issued on a showing of probable cause and no record was required to be made of what had been seized."); *see* Brian Frazelle & David Gray, *What the Founders Would Say About Cellphone Surveillance*, ACLU (Nov. 17, 2017), https://www.aclu.org/news/privacy-technology/what-founders-would-say-about-cellphone-surveillance [https://perma.cc/23EY-VJFB] (mentioning another English case, *Wilkes v. Wood*, where the court "condemned general warrants as 'totally subversive of the liberty of the subject' because they gave officers 'a discretionary power . . . to search wherever their suspicions may chance to fall'" (alteration in original) (quoting Wilkes v. Wood, (1763) 98 Eng. Rep. 489, 498 (K.B.))).

31 Boyd v. United States, 116 U.S. 616, 626–27 (1886) ("[I]t may be confidently asserted that its propositions were in the minds of those who framed the [F]ourth [A]mendment to the [C]onstitution, and were considered as sufficiently explanatory of what was meant by unreasonable searches and seizures.").

32 U.S. CONST. amend. IV.

33 *Probable Cause*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/probable_cause [https://perma.cc/22KM-WKPD]; *see* Illinois v. Gates, 462 U.S. 213, 238 (1983).

34 *The Search Warrant Requirement in Criminal Investigations & Legal Exceptions*, JUSTIA, https://www.justia.com/criminal/procedure/warrant-requirement [https://perma.cc/787P-5C4U] (Oct. 2022); Maryland v. Garrison, 480 U.S. 79, 84 (1987) ("[T]he scope of a lawful search is 'defined by the object of the search and the places in which there is probable cause to believe that it may be found.'" (quoting United States v. Ross, 456 U.S. 798, 824 (1982))).

35 United States v. Chatrie, 590 F. Supp. 3d 901, 928 (E.D. Va. 2022) ("[A] warrant must 'confine the executing [officers'] discretion by allowing them to seize only evidence of a particular crime.'" (second alteration in original) (quoting United States v. Cobb, 970 F.3d 319, 328 (4th Cir. 2020))).

36 *The Search Warrant Requirement in Criminal Investigations & Legal Exceptions*, *supra* note 34.

37 389 U.S. 347 (1967).

B. *Fourth Amendment Searches and the Reasonable Expectation of Privacy*

Katz v. United States was a landmark Supreme Court decision that expanded the Fourth Amendment's protections against unreasonable searches and seizures.[38] It did so by holding that a Fourth Amendment search occurs when the government intrudes upon an individual's reasonable expectation of privacy.[39] In *Katz*, the government placed an electronic listening and recording device on the outside of a public telephone booth to eavesdrop on the defendant's calls.[40] The Court held that the Fourth Amendment protects people, not places, so it did not matter that the defendant's conversations took place in a public telephone booth.[41] What mattered was that the government's activities violated the defendant's privacy and thus constituted a search under the Fourth Amendment.[42]

Justice Harlan's influential concurrence in *Katz* introduced a two-part test, known as the *Katz* test, which is now used to determine whether a law enforcement official has violated an individual's reasonable expectation of privacy.[43] The first part of the test requires that a person has shown a subjective expectation of privacy.[44] The second requirement is that society must find the expectation of privacy to be reasonable.[45] Both prongs of the test must be met for a law enforcement official's action to be considered a Fourth Amendment search.[46] The *Katz* test has been used for decades but has attracted criticism in recent years in the face of modern technologies.[47] Critics argue that new technologies make it more difficult for courts to assess whether an expectation of privacy should be considered reasonable.[48]

---

38 *See* Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018); U.S. CONST. amend. IV; *Katz*, 389 U.S. 347.

39 *Katz*, 389 U.S. at 353; *see Fourth Amendment*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/fourth_amendment [https://perma.cc/WA6W-RUDR] (May 2023).

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

41 *Id.* at 351–52.

42 *Id.* at 353.

43 *Id.* at 361 (Harlan, J., concurring); *see* Michael Brewster, Note, *Policing the Police: Utilizing the Right to Record and Civilian Oversight Boards to Monitor Police Activity in the United States*, 88 BROOK. L. REV. 993, 1006 (2023).

44 *Katz*, 389 U.S. at 361.

45 *Id.*

46 *Id.*

47 *See* sources cited *infra* note 88.

48 *See* sources cited *infra* note 88.

C. *The Third-Party Doctrine*

The third-party doctrine holds that an individual does not have a legitimate expectation of privacy in information that they voluntarily provide to a third party.[49] Therefore, the government is able to access that information without a warrant.[50] The third-party doctrine was first introduced in *United States v. Miller*, a case in which the Supreme Court held that bank records are not protected under the Fourth Amendment.[51] The defendant in *Miller* was convicted of possessing unregistered alcohol distilling equipment and operating a distilling business without paying the whiskey tax.[52] Government agents issued subpoenas to the presidents of two banks, which required them to produce all records of Miller's accounts.[53] Miller filed a motion to suppress the bank documents, claiming that they were illegally seized.[54] The Court held that Miller did not have a Fourth Amendment interest in the contents of the bank records.[55] The checks were used for commercial transactions and therefore were not confidential.[56] All of the information in the documents was "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[57]

In *Smith v. Maryland*, the Supreme Court expanded the third-party doctrine, holding that the installation and use of a pen register did not violate the Fourth Amendment.[58] The defendant in *Smith* had robbed a Maryland woman and repeatedly threatened her through telephone calls.[59] The police noticed a man who fit the description of the offender driving through the woman's neighborhood and traced his license plate.[60] The man was identified as Smith, and the police directed a telephone company to install a pen register at its offices to record the numbers that were dialed from Smith's home.[61] The register showed that Smith had contacted the woman in the past, and he was arrested after further

---

49 John Villasenor, *What You Need to Know About the Third-Party Doctrine*, THE ATLANTIC (Dec. 30, 2013), https://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721 [https://perma.cc/J5HK-P4UY].

50 *Id.*

51 425 U.S. 435, 437 (1976).

52 *Id.* at 436.

53 *Id.* at 437–38.

54 *Id.* at 438.

55 *Id.* at 442.

56 *Id.*

57 *Id.*

58 442 U.S. 735, 745–46 (1979).

59 *Id.* at 737.

60 *Id.*

61 *Id.*

investigation.[62] Smith filed a motion to suppress all evidence derived from the pen register on the basis that the police had failed to obtain a warrant prior to its installation.[63] The Court held that Smith did not have a legitimate expectation of privacy regarding the numbers that he dialed on his phone.[64] The Court reasoned that telephone users generally know that they must communicate the telephone numbers they dial to the telephone company in order to make calls, that the telephone company has facilities that record this information, and that the telephone company records this information for legitimate business purposes, such as detecting fraud.[65] Therefore, the installation and use of the pen register was not a search under the Fourth Amendment, and a warrant was not required.[66]

The rapid proliferation of new technologies has complicated the application of the third-party doctrine because it is unclear what constitutes voluntary disclosure in these contexts.[67] Furthermore, the amount of sensitive information shared through these technologies has increased exponentially, raising questions about the scope of the third-party doctrine and its compatibility with modern conceptions of privacy.[68] The question of whether the third-party doctrine applies to search history data has not yet been answered.[69]

D. *Particularity:* Ybarra v. Illinois

A question that arises in the context of keyword search warrants is whether they satisfy the particularity requirement of the Fourth Amendment.[70] The seminal case regarding particularity is *Ybarra v.*

---

62 *Id.*

63 *Id.*

64 *Id.* at 742.

65 *Id.* at 742–43.

66 *Id.* at 745–46.

67 *See* Note, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924, 1928–30 (2017).

68 *See id.* at 1938–41.

69 Although the Supreme Court has not ruled on whether the third-party doctrine applies to search history data, some of the Justices have expressed concern about the continued application of the doctrine. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (stating that the third-party doctrine 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"); Carpenter v. United States, 138 S. Ct. 2206, 2262 (2018) (Gorsuch, J., dissenting) ("[T]he 'third-party doctrine is not only wrong, but horribly wrong.'" (quoting Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 564 (2009))).

70 *See* Tim Cushing, *Colorado Supreme Court to Hear Challenge of Reverse Keyword Warrant Served to Google*, TECHDIRT (Feb. 3, 2023, 12:07 PM), https://www.techdirt.com/2023/02/03/colorado-supreme-court-to-hear-challenge-of-reverse-keyword-warrant-served-to-google

Illinois, which stands for the proposition that an individual's proximity to someone who is suspected of criminal activity does not create probable cause to search that individual.[71] In *Ybarra*, a search warrant was issued for police officers to search a tavern and its bartender for drugs.[72] One of the officers conducted pat-downs of all the customers who were in the tavern, including Ybarra.[73] The police found heroin in Ybarra's pocket, and he was charged with unlawful possession of a controlled substance.[74] The Supreme Court held that the search was unconstitutional because probable cause must be particularized as to each individual that the government wishes to search or seize.[75] The search warrant had only given the officers the authority to search the tavern and its bartender; they could not search Ybarra simply because he was in the tavern at the time the search warrant was executed.[76] As the officers knew nothing in particular about the defendant that would suggest his involvement in criminal activity, the search of his person was deemed by the Court to violate the Fourth Amendment.[77]

E. *Digital Privacy:* Carpenter v. United States

The Supreme Court's most recent case on the Fourth Amendment and digital privacy is *Carpenter v. United States*.[78] *Carpenter* was a landmark case in which the Court considered whether the government violates the Fourth Amendment when it accesses an individual's cell-site location information (CSLI) without a warrant.[79] In *Carpenter*, police officers arrested four men suspected of robbing Radio Shack and T-Mobile stores.[80] The prosecutors were able to identify the defendant,

---

[https://perma.cc/CM2A-HDZR] ("Some courts lean towards a more traditional definition of terms like 'particularity,' which means cops need to narrow down their list of suspects before asking a third party to hand over a massive amount of (untargeted) data. Other courts feel the particularity requirement only attaches after law enforcement has received data from Google.").

71 444 U.S. 85, 91 (1979) ("[A] person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person.").

72 *Id.* at 88.

73 *Id.*

74 *Id.* at 89.

75 *Id.* at 91 (reiterating that the Fourth Amendment "protect[s] the 'legitimate expectations of privacy' of persons, not places" (first quoting Rakas v. Illinois, 439 U.S. 128, 138–43, 148–49 (1978); and then citing Katz v. United States, 389 U.S. 347, 351–52 (1967))).

76 *Id.* at 91–92.

77 *Id.* at 90–91, 96.

78 138 S. Ct. 2206 (2018).

79 Cell phones are constantly connecting to cell sites in order to work, and each connection generates a time-stamped record known as cell-site location information. *Id.* at 2211.

80 *Id.* at 2212.

Timothy Carpenter, based on information obtained from one of the suspects.[81] Two orders were issued directing Carpenter's phone carriers to produce CSLI for his telephone.[82] The first order requested 152 days of CSLI from MetroPCS, and the second order requested seven days of CSLI from Sprint.[83] From these orders, the government received 12,898 location points.[84] Carpenter was convicted after his CSLI revealed that his phone was near four of the robberies when they occurred.[85] The *Carpenter* Court declined to extend the third-party principle of *Smith* and *Miller*; instead, it held that a search occurs when the government obtains seven days' worth of an individual's CSLI.[86] The Court acknowledged that its ruling was narrow, and although it decided that an individual has a reasonable expectation of privacy in their CSLI, it left open the question of whether other types of digital information, such as search history data, are protected under the Fourth Amendment.[87]

Many legal scholars suggest that the *Katz* test should be replaced, and one main reason is because advancements in technology may change society's expectations of privacy.[88] A new Fourth Amendment test emerged from the *Carpenter* decision, and arguments have been made for that test to replace the *Katz* test.[89] In *Carpenter*, the Court engaged in a balancing test to determine whether a warrant is necessary when the government wants to acquire data from digital technologies.[90] The

---

81 *Id.*

82 *Id.*

83 *Id.*

84 *Id.*

85 *Id.* at 2212–13.

86 *Id.* at 2216–20, 2217 n.3.

87 *Id.* at 2220.

88 *See, e.g.*, LAURA HECHT-FELELLA, BRENNAN CTR. FOR JUST., THE FOURTH AMENDMENT IN THE DIGITAL AGE: HOW *CARPENTER* CAN SHAPE PRIVACY PROTECTIONS FOR NEW TECHNOLOGIES (2021), https://www.brennancenter.org/media/7399/download [https://perma.cc/K8W8-446P]; Matthew Tokson & Paul Ohm, Carpenter *Should Replace* Katz *in Fourth Amendment Law*, LAWFARE (July 13, 2022, 8:01 AM), https://www.lawfareblog.com/carpenter-should-replace-katz-fourth-amendment-law [https://perma.cc/U2K4-S3MS]; Margaret Hu, *Cybersurveillance Intrusions and an Evolving* Katz *Privacy Test*, 55 AM. CRIM. L. REV. 127, 129 (2018); Joshua Schow, Student Work, *Defying Expectations: A Case for Abandoning* Katz *by Adopting a Digital Trespass Doctrine*, 49 STETSON L. REV. 339, 340 (2020); Colin Shaff, Note, *Is the Court Allergic to* Katz*? Problems Posed by New Methods of Electronic Surveillance to the "Reasonable-Expectation-of-Privacy" Test*, 23 S. CAL. INTERDISC. L.J. 409, 448 (2014); John P. Jarecki, Comment, *Privacy in the Panopticon: The Fourth Amendment Case Against Perpetual Surveillance*, 48 U. DAYTON L. REV. 41, 59–60 (2022); Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139, 159 (2016); Matthew Tokson, *The* Carpenter *Test as a Transformation of Fourth Amendment Law*, 2023 U. ILL. L. REV. 507, 512–13, 515 (2023).

89 *See* Tokson & Ohm, *supra* note 88.

90 *Carpenter*, 138 S. Ct. 2206.

majority's five-factor analysis considered "intimacy, comprehensiveness, expense, retrospectivity, and voluntariness."[91]

For the intimacy factor, the Court looked to the nature of the information sought.[92] A person is more likely to have a reasonable expectation of privacy if the technology provides law enforcement officials with intimate details about one's life.[93] Comprehensiveness, the second factor, refers to the "depth, breadth, and comprehensive reach" of the information that is disclosed.[94] The expense factor compares the cost of obtaining the data using the new technology with the cost of obtaining the data using traditional investigative tools.[95] The Court found it troubling that, unlike in the past, the government can now collect extensive information about an individual at little to no expense.[96] In the pre-technological world, it was inconceivable that the government would be able to obtain information about an individual for an extended period of time without a tremendous expenditure of resources.[97] Allowing the government to track individuals by using their CSLI is contrary to society's expectations, so a warrant is needed.[98] The retrospectivity factor asks whether the technology provides law enforcement officials with information that is otherwise unknowable.[99] The retrospective quality of CSLI is problematic because it allows for the government to track the past locations of all cell phone users.[100] The current ability of the government to obtain retrospective data goes against society's expectations because the government would not have been able to go back in time to retrace an

91 *Id.* at 2234 (Kennedy, J., dissenting) (characterizing the majority's analysis).

92 *Id.* at 2217–18 (majority opinion); *see* Matthew Tokson, *The Aftermath of* Carpenter*: An Empirical Study of Fourth Amendment Law, 2018–2021*, 135 HARV. L. REV. 1790, 1801 (2022).

93 *Carpenter*, 138 S. Ct. at 2217 (finding a reasonable expectation of privacy in an individual's CSLI because it contains the "privacies of life" and "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations'" (first quoting Riley v. California, 573 U.S. 373, 403 (2014); and then quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring))); *see* HECHT-FELELLA, *supra* note 88, at 9–10.

94 There is an expectation of privacy when the information creates a record that is "detailed, encyclopedic, and effortlessly compiled." *Carpenter*, 138 S. Ct. at 2216–17, 2223.

95 *Id.* at 2217–18.

96 *Id.* at 2218.

97 *Id.* at 2217 ("Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so 'for any extended period of time was difficult and costly and therefore rarely undertaken.'" (quoting *Jones*, 565 U.S. at 429 (Alito, J., concurring))).

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

99 *Id.* at 2218.

100 *Id.* ("[T]his newfound tracking capacity runs against everyone. . . . [P]olice need not even know in advance whether they want to follow a particular individual, or when.").

individual's steps in the past.[101] The last factor is voluntariness, which looks at whether the information was voluntarily conveyed to a third party.[102] Information is not voluntarily shared if the technology is needed to participate in daily life and if the collection of information is "inescapable and automatic."[103] These five factors can be used to determine whether a warrant is required to obtain search history data.[104]

F. *Publicly Known Uses of Keyword Search Warrants*

Law enforcement officials currently use keyword search warrants to obtain search history data.[105] Not much is known about keyword search warrants since they are typically used in secret, but they have recently gained a great deal of public attention.[106] What is known about these warrants is that they are overly broad and can turn innocent web users into criminal suspects.[107] The earliest known publicly revealed keyword search warrant is from 2017.[108] In Minnesota, a man had created a fake ID and used it to receive a $28,500 wire transfer from a bank.[109] The keyword search warrant asked Google to provide the information of everyone who had searched for any of four variations of the true bank account owner's name between December 1, 2016, and January 7, 2017.[110] The government sought the names, addresses, telephone numbers, dates of birth, social security numbers, email addresses, payment information, account information, Internet Protocol (IP) addresses, and MAC

101 *Id.* ("In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts . . . .").

102 *Id.* at 2219–20.

103 *Id.* at 2220, 2223.

104 *See* HECHT-FELELLA, *supra* note 88, at 9.

105 *See id.* at 29.

106 *See* Brewster, *Exclusive*, *supra* note 14.

107 *See* Gilens, Lynch & Alimonti, *supra* note 23.

108 The name of the case is unknown. *See* Brewster, *Exclusive*, *supra* note 14.

109 Thomas Brewster, *Cops Demand Google Data on Anyone Who Searched a Person's Name . . . Across a Whole City*, FORBES (Mar. 17, 2017, 7:15 AM), https://www.forbes.com/sites/thomasbrewster/2017/03/17/google-government-data-grab-in-edina-fraud-investigation/?sh=36b7047f7ade [https://perma.cc/8H9C-5E4B].

110 *Id.*

addresses[111] of the people who performed the searches.[112] The keyword search warrant stated that the law enforcement official applied for the warrant because the requested information "constitute[d] evidence which tends to show a crime has been committed, or tends to show that a particular person has committed a crime."[113] The judge found that probable cause existed on that basis and approved the warrant.[114]

In 2018, a serial bomber built and planted six explosive devices that killed two people and injured four others in Austin, Texas.[115] The Federal Bureau of Investigation (FBI) served three keyword search warrants on Google.[116] The warrants asked for information about users who searched for certain terms and addresses on Google Search, Google Maps, Waze, and YouTube.[117] They stated that there was probable cause that the individuals who searched for those terms and addresses would help law enforcement identify those who knew about the bombing.[118] The police investigation resulted in the identification of the perpetrator, a twenty-three-year-old man named Mark Anthony Conditt.[119]

---

111 A Media Access Control (MAC) address is a twelve-digit number that is used to uniquely identify every device connected on a network. *What's a MAC Address and How Do I Find It?*, OHIO STATE UNIV. (Jan. 16, 2021), https://slts.osu.edu/articles/whats-a-mac-address-and-how-do-i-find-it [https://perma.cc/TM3R-8N3G].

112 Application for Search Warrant, No. 27-CR-CV-17-1 (Minn. Dist. Ct. Feb. 1, 2017), https://s3.documentcloud.org/documents/3519211/Edina-Police-Google-Search-Warrant-Redacted.pdf [https://perma.cc/AQG2-VZ2S].

113 *Id.* at 2.

114 Tony Webster, *Minnesota Judge Signs a Search Warrant for Personal Information on Anyone Who Googled Someone's Name*, TONY WEBSTER (Mar. 9, 2017), https://tonywebster.com/journalism/minnesota-judge-signs-a-search-warrant-for-personal-information-on-anyone-who-googled-someones-name [https://perma.cc/Q6K5-UW2D].

115 *Inside the FBI's Race to Stop Austin, Texas, Bombing Spree*, CBS NEWS (Oct. 20, 2020, 11:02 PM), https://www.cbsnews.com/news/austin-serial-bomber-mark-conditt-fbi-declassified [https://perma.cc/74TS-PFHY].

116 Microsoft and Yahoo also received a keyword search warrant. Brewster, *Exclusive*, *supra* note 14.

117 Affidavit ¶ 1, *In re* the Search of Info. & Recs. Associated with Google Searches for Various Search Terms That Are Stored at Premises Controlled by Google, No. 1:18-mj-170 (W.D. Tex. Mar. 14, 2018) [hereinafter March 14 Affidavit]; Affidavit ¶ 1, *In re* the Search of Info. & Recs. Associated with Google Searches for Various Search Terms That Are Stored at Premises Controlled by Google (2), No. 1:18-mj-191 (W.D. Tex. Mar. 19, 2018) [hereinafter First March 19 Affidavit]; Affidavit ¶ 1, *In re* the Search of Info. & Recs. Associated with Google Searches for Various Search Terms That Are Stored at Premises Controlled by Google (3), No. 1:18-mj-189 (W.D. Tex. Mar. 19, 2018) [hereinafter Second March 19 Affidavit].

118 March 14 Affidavit, *supra* note 117, ¶ 6; First March 19 Affidavit, *supra* note 117, ¶ 7; Second March 19 Affidavit, *supra* note 117, ¶ 6.

119 *Inside the FBI's Race to Stop Austin, Texas, Bombing Spree*, *supra* note 115.

Another keyword search warrant was authorized on June 15, 2020.[120] In *United States v. Williams*, an associate of the disgraced R&B singer R. Kelly was sentenced to eight years in prison for setting fire to a rental car in front of a house in Florida where the victim was staying.[121] The warrant was served on Google and requested information about users who had searched for the address of the home around the time of the arson.[122] Law enforcement officials received the IP addresses of the users, and the results showed that one individual had searched for the address three times in the days leading up to the arson.[123] The IP address was connected to a telephone number in Georgia that belonged to Michael Williams, a family member of a former publicist of R. Kelly.[124] From there, investigators were able to determine that the device was at the location of the crime when it occurred.[125] Later that year, in October and November of 2020, three keyword search warrants were submitted to Google, resulting in the case of *People v. Seymour*.[126]

In September 2021, the Justice Department accidentally unsealed a keyword search warrant, which was executed in connection with a 2019 investigation relating to the trafficking and sexual abuse of a minor.[127] The warrant was issued to Google and requested the Google account information and IP addresses of anyone who searched for the victim's name, two spellings of her mother's name, or her address, over a period of sixteen days.[128] The document has been sealed again, and full details of the case have not been published in order to protect the identities of the minor and her family.[129]

---

120 Affidavit in Support of an Application for a Search Warrant ¶ 17, *In re* the Search of Info. Associated with the Cellular Device Assigned Call No. (229) 418-8231, That Is Stored at Premises Controlled by T-Mobile, No. 20-MC-1584 (E.D.N.Y. July 13, 2020).

121 Nina Pullano, *R. Kelly Associate Gets 8 Years for Setting Fire Outside a Victim's Home*, COURTHOUSE NEWS SERV. (Nov. 17, 2021) https://www.courthousenews.com/r-kelly-associate-gets-8-years-for-setting-fire-outside-a-victims-home [https://perma.cc/3GXV-F67J]; *see* United States v. Williams, No. 20-cr-00395 (E.D.N.Y. 2020).

122 Siladitya Ray, *Google Shared Search Data with Feds Investigating R. Kelly Victim Intimidation Case*, FORBES (Oct. 9, 2020, 11:24 AM), https://www.forbes.com/sites/siladityaray/2020/10/08/google-shared-search-data-with-feds-investigating-r-kelly-victim-intimidation-case/?sh=2039988d7c62 [https://perma.cc/54Q9-67AN].

123 Affidavit in Support of an Application for a Search Warrant, *supra* note 120, ¶ 17.

124 *Id.*; 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, 7:59 AM), https://www.businessinsider.com/google-can-give-police-keyword-data-from-search-histories-2020-10 [https://perma.cc/QXU3-8CEY].

125 Hamilton, *supra* note 124.

126 Motion to Suppress, *supra* note 9, ¶¶ 22–23, 25.

127 Brewster, *Exclusive*, *supra* note 14.

128 *Id.*

129 *Id.*

G. *Google's Process in Responding to a Keyword Search Warrant*

Although many details about keyword search warrants remain undisclosed to the public, Google has recently shed light on the procedures it follows upon receiving such warrants from law enforcement officials.[130] After Google receives a keyword search warrant from a law enforcement official, it creates a text-based query that is run over its records of searches performed using Google services.[131] The results are de-identified and then produced to law enforcement.[132] The data that is handed over includes: (1) the date and time the search was conducted; (2) the coarse location information;[133] (3) the user's search query; (4) the result of the user's search query; (5) the host or Google domain name that was used; (6) the part of the URL that follows the host; (7) the shortened version of a GAIA ID if the search was made by someone who was signed into a Google Account, or the shortened version of a Browser Cookie ID if the search was made by someone who was not signed into a Google Account;[134] and (8) the associated user agent string.[135]

The requirements of a keyword search warrant can vary; if a warrant only requests an exact phrase, Google will only create and run a query for that exact phrase.[136] However, it is possible and more common that the warrant forces Google to produce every query containing the phrase.[137] In this situation, other terms or phrases may appear along with the requested phrase.[138] Law enforcement officials have the discretion to

---

130 *See* Declaration of Legal Investigations Support Analyst, *supra* note 6, ¶¶ 2–10.

131 *Id.* ¶ 4.

132 *Id.* ¶¶ 7–8.

133 Coarse location information is information that provides the approximate location of a user or device. *Location Data*, GOOGLE MAPS PLATFORM, https://developers.google.com/maps/documentation/android-sdk/location [https://perma.cc/5LNU-CHL2]. Google infers this information from the IP address that was used when the user conducted the search. Declaration of Legal Investigations Support Analyst, *supra* note 6, ¶ 7.

134 A Google Legal Investigations Support analyst de-identifies the results by truncating either the GAIA ID or the Browser Cookie ID, as applicable. Declaration of Legal Investigations Support Analyst, *supra* note 6, ¶ 7.

135 *Id.* A user agent string is a line of text that identifies the browser and operating system being used to the web server. Chris Hoffman, *What Is a Browser's User Agent?*, HOW-TO GEEK (Sept. 13, 2017, 11:52 AM), https://www.howtogeek.com/114937/htg-explains-whats-a-browser-user-agent [https://perma.cc/HMG8-WZWZ].

136 Declaration of Legal Investigations Support Analyst, *supra* note 6, ¶ 6.

137 *Id.*

138 For example, a keyword search warrant may request that Google produce every query that includes a specific house number and street name. *See id.* The results may include queries containing the cities, states, and zip codes that were searched along with the house number and street name. *See id.*

determine which search results are pertinent to their investigation.[139] For example, if multiple users search for a partial address at around the same time, the officials can decide to exclude the searches if they are addresses in a city or state not relevant to the investigation.[140]

After the government reviews the results of the query and if the initial warrant authorizes it, the government can compel Google to produce more information about the users from the de-identified results.[141] If a responsive user was logged into a Google account at the time of the search, Google will provide the law enforcement officials with the IP address associated with the search, the full GAIA ID, and the basic subscriber information for that GAIA ID.[142] If a responsive user was not logged into a Google account at the time of the search, Google will provide the officials with the IP address associated with the search and the full Browser Cookie ID.[143] If the initial warrant does not authorize the government officials to obtain identifying information about the responsive users, they can apply for another warrant to receive such information from Google.[144]

The number of search warrants the government has sent to Google has dramatically increased throughout the years.[145] From July 2022 to December 2022, Google received 30,442 search warrants from the government, whereas from July 2012 to December 2012, Google only received 1,896 search warrants.[146] Despite Google's support for banning keyword search warrants, it has produced some data for eighty-four percent of all search warrant requests between July 2022 and December 2022.[147] These statistics and the disclosure of Google's procedures regarding keyword search warrants shed light on the company's cooperation with law enforcement.[148]

---

139 *Id.* ¶ 8.

140 *Id.*

141 *Id.* ¶¶ 8–9.

142 *Id.* ¶ 9.

143 *Id.*

144 *Id.*

145 *See Global Requests for User Information*, GOOGLE TRANSPARENCY REP., https://transparencyreport.google.com/user-data/overview?user_requests_report_period=authority:US (last visited July 24, 2023).

146 *Id.*

147 *Id.*; *see* Zack Whittaker, *Google, Microsoft and Yahoo Back New York Ban on Controversial Search Warrants*, TECHCRUNCH (May 10, 2022, 8:07 AM), https://techcrunch.com/2022/05/10/google-new-york-geofence-keyword-warrant [https://perma.cc/Y24R-CKFR].

148 *See Global Requests for User Information*, *supra* note 145; Declaration of Legal Investigations Support Analyst, *supra* note 6, ¶¶ 2–10.

H. *Geofence Warrants:* United States v. Chatrie

A geofence[149] warrant is another type of reverse search warrant that Google receives, and it demands the identification of every device in a certain area during a particular time period.[150] Keyword search warrants and geofence warrants are similar in that they are both used by law enforcement to compel companies, such as Google, to help them find suspects.[151] *People v. Seymour* is currently the only case that has addressed the constitutionality of keyword search warrants, but there have been several cases where geofence warrants were found to be unconstitutional.[152] One such case is *United States v. Chatrie*, which involved a bank robbery in Virginia.[153] A detective served a geofence warrant to Google after viewing the bank's surveillance footage, which showed the perpetrator with a phone in his hand.[154] He believed that Google would have the requested information since many mobile devices, especially those using the Android operating system, are connected to Google accounts and have Google location services enabled.[155] The warrant requested the location information for every device within the geofence from 4:20 p.m. to 5:20 p.m. on the day that the robbery occurred.[156] Google produced location data in accordance with the warrant, which led the police to Okello Chatrie.[157] After Chatrie was charged, he filed a motion to suppress the evidence derived from the geofence warrant.[158] The district court denied the motion, but it held that

---

149 A geofence is a virtual boundary around a specific geographic location. *What Is a Geofence?*, VERIZON CONNECT, https://www.verizonconnect.com/glossary/what-is-a-geofence [https://perma.cc/X87L-9R7R]; Rahul Awati, *Geofencing*, TECHTARGET, https://www.techtarget.com/whatis/definition/geofencing [https://perma.cc/4LY3-GN9Q].

150 *See* Guariglia, *supra* note 6; Motion to Suppress, *supra* note 9, ¶ 11 ("A geofence warrant is a type of reverse warrant that searches all Google users with 'Location History' enabled for all devices in a given area."); United States v. Chatrie, 590 F. Supp. 3d 901, 914 (E.D. Va. 2022) (explaining that a geofence warrant "(1) identifies a geographic area (also known as the 'geofence,' often a circle with a specified radius), (2) identifies a certain span of time, and (3) requests Location History data for all users who were within that area during that time"). The time frame could range from a few minutes to a few hours. *Chatrie*, 590 F. Supp. 3d at 914.

151 Bhuiyan, *supra* note 8.

152 Lynch & Crocker, *supra* note 18; Corbly, *supra* note 6; *see also* Jennifer Lynch, *First Court in California Suppresses Evidence from Overbroad Geofence Warrant*, ELEC. FRONTIER FOUND. (Oct. 11, 2022), https://www.eff.org/deeplinks/2022/10/california-court-suppresses-evidence-overbroad-geofence-warrant [https://perma.cc/7YF8-REPZ].

153 590 F. Supp. 3d 901.

154 *Id.* at 906, 917.

155 *Id.* at 920. Chatrie was using an Android device at the time of the robbery. *Id.* at 910 n.13.

156 *Id.* at 919.

157 *Id.* at 906.

158 *Id.*

the geofence warrant lacked particularized probable cause and therefore violated the Fourth Amendment.[159] Part II will argue that keyword search warrants should be deemed unconstitutional on the same grounds.[160]

II. ANALYSIS

A. *The* Carpenter *Test and Search Histories*

Keyword search warrants should be deemed unconstitutional because the government's acquisition of search history data is a Fourth Amendment search that requires a traditional search warrant.[161] Courts have used the *Katz* test for decades to determine whether a search has occurred, but the two-prong test is inadequate for protecting individuals' Fourth Amendment rights in today's ever-evolving technological landscape.[162] Instead, courts should consider the *Carpenter* test's five factors in determining whether an individual has a reasonable expectation of privacy in the data acquired from new technologies.[163] An application of the test shows that individuals have a reasonable expectation of privacy in their search history data.[164] Keyword search warrants violate that expectation and should be held unconstitutional.[165] Each factor of the *Carpenter* test supports a finding that law enforcement officials need a traditional search warrant to obtain search history data.[166]

1. Intimacy

A traditional search warrant should be required to obtain search history data because, similar to CSLI, search history data can provide law enforcement with personal details of an individual's life.[167] A person's Google search can reveal their most intimate thoughts, which they may not feel comfortable sharing with even the people closest to them.[168] In

159 *Id.* at 925.

160 *See infra* Part II.

161 *See* Motion to Suppress, *supra* note 9, ¶ 36.

162 *See* Tokson & Ohm, *supra* note 88.

163 *See* HECHT-FELELLA, *supra* note 88, at 3; Carpenter v. United States, 138 S. Ct. 2206 (2018).

164 *See Carpenter*, 138 S. Ct. 2206.

165 *See* Motion to Suppress, *supra* note 9, ¶ 36.

166 *See Carpenter*, 138 S. Ct. 2206.

167 *See* Brewster, *Warrants Can Force Google*, *supra* note 5.

168 *See* Hidden Brain, *What Our Google Searches Reveal About Who We Really Are*, NPR (May 1, 2017, 9:01 PM), https://www.npr.org/2017/05/01/526399881/what-our-google-searches-reveal-about-who-we-really-are [https://perma.cc/3DQ5-5VP4].

2021, the top trending Google searches that began with "how to be" included: "How to be happy alone," "How to be a good kisser," and "How to be happy with yourself."[169] Google is easily accessible; cell phones are usually brought everywhere a person goes, which in turn allows the owner to be able to conduct searches from anywhere.[170] Individuals can use Google for hours a day, and in doing so, search history records are created that can reveal information that users do not want others to know.[171] Keyword search warrants have the potential to disclose personal facts about one's life that go beyond legitimate government interest.[172] The government's collection of an individual's search history data constitutes a search under the Fourth Amendment because it violates their reasonable expectation of privacy.[173]

One's search history can reveal a lot about a person and can even be used to identify them.[174] In 2006, AOL released twenty million web search queries from 650,000 of its users on its website.[175] Although the names of the users were replaced with numeric IDs, *The New York Times* was able to use the data to identify and locate user No. 4417749, Thelma Arnold, with ease.[176] Thelma had conducted hundreds of searches over the span of three months; her searches included "60 single men," "nicotine effects on the body," and "bipolar."[177] Other users' searches also seemed to be quite personal.[178] User No. 3505202 searched for "depression and medical leave," and user No. 7268042 searched for "fear that spouse

---

169 *Year in Search 2021*, GOOGLE TRENDS, https://trends.google.com/trends/yis/2021/US [https://perma.cc/LPG4-334Z].

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

171 A survey of 1,000 Americans found that seventy-one percent of respondents would be embarrassed if someone they knew could see everything that they had ever searched. Aseem Kishore, *Survey: The Internet Habits Americans Are Hiding*, ONLINE TECH TIPS (Aug. 1, 2022), https://www.online-tech-tips.com/fun-stuff/internet-habits-americans-hide [https://perma.cc/2PB9-7YPH]; *see* Brian X. Chen, *It's Google's World. We Just Live in It.*, N.Y. TIMES (May 3, 2021), https://www.nytimes.com/2020/10/20/technology/doj-google.html [https://archive.ph/DsHkS].

172 *See* Kishore, *supra* note 171; Lindsey R. Mattson, The *Carpenter* Shift: The Evolution of Fourth Amendment Jurisprudence in the Digital Age 46 (May 2022) (B.A. thesis, Trinity College), https://digitalrepository.trincoll.edu/cgi/viewcontent.cgi?article=2003&context=theses [https://perma.cc/JFT9-YBTG]; Orin S. Kerr, *Implementing* Carpenter, *in* THE DIGITAL FOURTH AMENDMENT (forthcoming), https://ssrn.com/abstract=3301257 [https://perma.cc/7ELS-VBWV].

173 Motion to Suppress, *supra* note 9, ¶ 45.

174 *See* Matthew Werner, Note, *Google and Ye Shall Be Found: Privacy, Search Queries, and the Recognition of a Qualified Privilege*, 34 RUTGERS COMPUT. & TECH L.J. 273, 280 (2007); Michael Barbaro & Tom Zeller Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES (Aug. 9, 2006), https://www.nytimes.com/2006/08/09/technology/09aol.html [https://web.archive.org/web/20230626042117/https://www.nytimes.com/2006/08/09/technology/09aol.html].

175 Barbaro & Zeller Jr., *supra* note 174.

176 *Id.*; *see* Werner, *supra* note 174, at 280.

177 Barbaro & Zeller Jr., *supra* note 174.

178 *See id.*

contemplating cheating."[179] Thelma's surprise at the fact that AOL had saved and published her data, and her plans to discontinue her AOL subscription, supports the idea that people expect privacy in their searches.[180] The outrage that ensued following the release of AOL's search query logs led to a class action lawsuit against AOL, which was settled for five million dollars in cash payments.[181] The intimate nature of search history data indicates that law enforcement officials need a traditional search warrant to collect such information.[182]

2. Comprehensiveness

The comprehensiveness of search history data further reinforces the necessity for law enforcement officials to secure a traditional search warrant prior to acquiring such information.[183] The comprehensiveness factor is concerned with the depth, breadth, and comprehensive reach of the information or, in other words, "the precision of the information, the duration of observation, and the number of people observed."[184] The information that Google has is precise: Google has been collecting and storing search history data since the company was created, and the data can reveal a detailed record of an individual's life.[185] Google and its subsidiaries, which include YouTube and Waze, offer services that

---

179 *Id.*

180 *See id.* Keyword search warrants can have chilling effects. They can discourage individuals from searching certain terms or from using search engines entirely. *See id.*

181 Paul Bond, *Court Grants Final Approval to Class Action Settlement over AOL's 2006 Anonymization Failure; Big Data Precursor Settles for Millions*, REED SMITH (May 30, 2013), https://www.technologylawdispatch.com/2013/05/big-data/court-grants-final-approval-to-class-action-settlement-over-aols-2006-anonymization-failure-big-data-precursor-settles-for-millions [https://perma.cc/64V8-YAKR]. The substantial settlement serves as compelling evidence that the release of the logs constituted a significant intrusion of privacy. *See id.*

182 *See* HECHT-FELELLA, *supra* note 88, at 9–10.

183 *See id.* at 9.

184 Matthew Tokson, *Inescapable Surveillance*, 106 CORNELL L. REV. 409, 422 (2021); *see* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018); Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 372–73 (2019).

185 Olivia Pym, *Google Keeps a Record of Everything You've Ever Searched (and Here's How to See It)*, ESQUIRE (Sept. 15, 2016), https://www.esquire.com/uk/life/news/a10690/google-record-everything-search-engine-history [https://perma.cc/8UZL-XF8R]; *see* Caleb, *How to Delete Your Google Search History*, EXPRESSVPN (Mar. 27, 2023), https://www.expressvpn.com/blog/how-to-permanently-delete-your-google-history [https://perma.cc/Y3YW-PT6F]; Caitlin Dewey, *Everything Google Knows About You (and How It Knows It)*, WASH. POST (Nov. 19, 2014, 7:07 AM) https://www.washingtonpost.com/news/the-intersect/wp/2014/11/19/everything-google-knows-about-you-and-how-it-knows-it [https://perma.cc/L5J7-YTYZ].

millions of individuals use.[186] With a single keyword search warrant, law enforcement officials can have Google comb through all of its users' search histories, spanning all of its various products and services.[187]

Duration is important to the comprehensiveness analysis because the longer the time frame, the more likely it is that sensitive information will be revealed.[188] In *Carpenter*, the Court found that accessing seven days of CSLI constituted a search under the Fourth Amendment.[189] In situations involving keyword search warrants, the government can compel Google to access months of search history data.[190] A great number of people are affected when these warrants are used.[191] Google Search has more than one billion monthly active users, and Google trawls through all of their search histories when it responds to a keyword search warrant.[192] These warrants enable law enforcement officials to effortlessly gather detailed information about numerous individuals over extended periods of time.[193]

3. Expense

New technologies allow law enforcement officials to gather detailed information about numerous individuals inexpensively.[194] In *Carpenter*, the Court had an issue with the fact that the government is able to access

---

186 Matthew Johnston, *7 Companies Owned by Google (Alphabet)*, INVESTOPEDIA, https://www.investopedia.com/investing/companies-owned-by-google [https://perma.cc/8BD4-AWNL] (Oct. 23, 2022). Google is the most visited website with roughly 87.6 billion visits in September 2022, followed by YouTube with around 69.1 billion visits in that same month. *Most Visited Websites by Traffic in the World for All Categories, September 2022*, SEMRUSH, https://www.semrush.com/website/top [https://perma.cc/XC8L-5QUE]. In 2022, Google Maps and Waze were the most popular mapping apps with about 24.7 million and 9.1 million downloads, respectively. *Leading Mapping Apps in the United States in 2022, by Downloads*, STATISTA (Feb. 7, 2023), https://www.statista.com/statistics/865413/most-popular-us-mapping-apps-ranked-by-audience [https://perma.cc/8YAC-9XRE].

187 *See, e.g.*, March 14 Affidavit, *supra* note 117 ¶¶ 1–2; First March 19 Affidavit, *supra* note 117 ¶¶ 1–2; Second March 19 Affidavit, *supra* note 117 ¶¶ 1–2; Gilens, Lynch & Alimonti, *supra* note 23.

188 *See* H. Brian Holland, *A Third-Party Doctrine for Digital Metadata*, 41 CARDOZO L. REV. 1549, 1591 (2020).

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

190 *See, e.g.*, First March 19 Affidavit, *supra* note 117 ¶ 6.

191 Individuals with Google accounts and individuals who do not have Google accounts are all affected by keyword search warrants. Declaration of Legal Investigations Support Analyst, *supra* note 6, ¶ 7.

192 Declaration of Legal Investigations Support Analyst, *supra* note 6, ¶ 4.

193 *See* HECHT-FELELLA, *supra* note 88, at 9.

194 *See id.* at 10.

a cell phone carrier's massive database of records at basically no cost.[195] The problem exists with keyword search warrants as well.[196] Law enforcement officials can obtain a warrant to request information from Google without having to expend the energy and money they otherwise would have if they were using traditional investigative tools.[197] In the pre-technological world, law enforcement officials would not be able to force a search engine to provide information on its users at all.[198] Now, a law enforcement official can easily obtain a warrant for this information.[199] A judge can approve a warrant in minutes and may not realize how many individuals will be affected.[200] Since society would not have expected these new police practices, a traditional search warrant is needed before Google provides law enforcement officials with its search history data.[201]

4. Retrospectivity

Society, prior to the digital age, would also not have expected that the government could trace anyone's past searches at any time.[202] The

---

195 Carpenter v. United States, 138 S. Ct. 2206, 2217–18 (2018).

196 *See* Legislative Memorandum from LatinoJustice PRLDEF, Supporting A.84/S.296 to Prohibit the Use of Reverse Warrants 1 (2022), https://www.nyclu.org/sites/default/files/220201-memo-latinojusticereversewarrant.pdf [https://perma.cc/3ZXR-PX9J].

197 *See* Legislative Memorandum from LatinoJustice PDRLDEF, *supra* note 196 ("By harnessing the limitless digital data troves collected and warehoused by the private technology industry, modern police departments can access millions of data points that together reveal 'the whole pattern of life' at a fraction of the cost of traditional surveillance programs." (footnote omitted) (quoting Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html [https://archive.ph/at9li])).

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

199 In *Chatrie*, a magistrate without a law degree signed the geofence warrant without asking the detective any questions. United States v. Chatrie, 590 F. Supp. 3d 901, 917–18 (E.D. Va. 2022).

200 *See* Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2513–14 (2021); Cahn & Humell, *supra* note 24 ("[J]udges who sign these orders do not know how many users will be caught up in the search at the time they approve them. They cannot because it is the keyword search itself that tells police how many individuals searched for a specific name, address, or product.").

201 *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (citing *Jones*, 565 U.S. at 430 (2012) (Alito, J., concurring)).

202 *See* HECHT-FELELLA, *supra* note 88, at 10; Motion to Suppress, *supra* note 9, ¶ 41 ("The U.S. Supreme Court has recently clarified how to identify a reasonable expectation of privacy in the digital context. Courts should look to 'historical understandings' of what was unreasonable at the nation's founding . . . . The Court has sought to preserve a 'degree of privacy against government that existed when the Fourth Amendment was adopted.' Consequently, the Court considers whether the 'retrospective quality' of the data gives the government access to a category of information that would be 'otherwise unknowable' before the digital age." (citation omitted) (first

retrospective quality of search history data is problematic because it enables law enforcement officials to access information that they would not know without a keyword search warrant.[203] In *Smith v. Maryland*, the data collection was prospective because the pen register had to be installed in order for the government to obtain the information.[204] In contrast, search history data is collected without a keyword search warrant; law enforcement officials apply for these warrants to access data that has already been collected.[205] Keyword search warrants allow the government to travel months into the past and can turn random people into suspects.[206] Therefore, the retrospectivity factor serves as an additional justification for requiring a traditional search warrant when the government wishes to obtain search history data.[207]

5. Voluntariness

The voluntariness factor also demonstrates that a traditional search warrant is necessary for the government to acquire search history data.[208] The third-party doctrine, which turns in large part on the idea of voluntariness, should not extend to such data.[209] The Supreme Court refused to apply the longstanding doctrine in *Carpenter v. United States* because the type of personal information in *Carpenter* was extremely different from the type of personal information in *Smith* and *Miller*.[210] The same can be said for an internet user's search history data.[211] *Smith* and *Miller* were decided in the 1970s, a time when search engines did not

---

quoting *Carpenter*, 138 S. Ct. at 2214; then quoting Kyllo v. United States, 533 U.S. 27, 34 (2001); and then quoting *Carpenter*, 138 S. Ct. at 2218)).

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

204 *See* Smith v. Maryland, 442 U.S. 735, 737 (1979).

205 *See* Pym, *supra* note 185.

206 First March 19 Affidavit, *supra* note 117, ¶ 6; Tim Cushing, *Reverse Keyword Warrant Challenged After Cops Asked Google to Search Millions of People's Data Multiple Times*, TECHDIRT (July 11, 2022, 9:38 AM), https://www.techdirt.com/2022/07/11/reverse-keyword-warrant-challenged-after-cops-asked-google-to-search-millions-of-peoples-data-multiple-times [https://perma.cc/PN4P-BX4G].

207 *See* HECHT-FELELLA, *supra* note 88, at 10.

208 *See id.* at 10.

209 *See id.* at 8.

210 Carpenter v. United States, 138 S. Ct. 2206, 2216–20 ("There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers . . . .").

211 The Court has recognized that an individual's search history is qualitatively different from physical records. Riley v. California, 573 U.S. 373, 395–96 (2014) ("[C]ertain types of data are . . . qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.").

exist.[212] Today, people can search for the answers to any question that they think of.[213] Their searches can reveal much about them and, similar to CSLI, can "provide[] an intimate window into a person's life."[214] The *Carpenter* Court emphasized that *Smith* and *Miller* considered the nature of the documents sought by the government when determining whether the defendants had a legitimate expectation of privacy in their contents.[215] Telephone logs, such as those produced from the pen register in *Smith*, do not reveal much about a person, and the business records in *Miller* were nonconfidential documents used in commercial transactions.[216] Therefore, the defendants in those cases had a limited expectation of privacy, and it was fine to subject those records to the third-party doctrine.[217] CSLI and search history data, on the other hand, are different because of their revealing nature; they both have the potential to create an extensive record of an individual's life.[218]

In Justice Marshall's dissent in *Smith*, he stated that an individual cannot assume the risk of the government having control of their information unless they had a choice in the matter.[219] He believed that individuals do not have a choice in accepting the risk of disclosure of their phone records because phones are necessary in an individual's life.[220] Similarly, the Court in *Carpenter* recognized the pervasiveness of modern technology in our everyday lives.[221] It held that Carpenter's CSLI was not shared voluntarily because cell phones are "indispensable to participation in modern society."[222] The same can be said for search engines.[223] The

---

212 *See Short History of Early Search Engines*, THE HISTORY OF SEO, https://www.thehistoryofseo.com/the-industry/short-history-of-early-search-engines [https://perma.cc/CW8S-BRSC].

213 Mohsin, *supra* note 25.

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

215 *Id.* at 2219.

216 *Id.* (first citing Smith v. Maryland, 442 U.S. 735, 742 (1979); then quoting *Riley*, 573 U.S. at 400; and then quoting United States v. Miller, 425 U.S. 435, 442 (1976)).

217 *Id.*

218 *Id.* at 2219–20.

219 *Smith*, 442 U.S. at 749 (Marshall, J., dissenting).

220 *Id.* at 749–50 ("Implicit in the concept of assumption of risk is some notion of choice. . . . [U]nless 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."); *see Digital Dragnets: Examining the Government's Access to Your Personal Data: Hearing Before the H.R. Comm. on the Judiciary*, 117th Cong. 18 (2022) (statement of Sarah Lamdan, Professor of Law, City University of New York School of Law) ("We may technically consent to driving on a public road, [or] we might click 'I agree' to access an online service . . . . But these choices are illusory. We must make them in order to participate in daily life.").

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

222 *Id.* (citing Riley v. California, 573 U.S. 373, 385 (2014)).

223 *See* Brief of Amicus Curiae Electronic Frontier Foundation in Support of Defendant's Motion to Suppress at 3, People v. Seymour, No. 21CR20001 (Colo. Dist. Ct. July 1, 2022),

internet holds a vast amount of valuable information, and search engines allow internet users to easily find the content they are looking for.[224] In fact, the average person uses Google Search three or four times per day.[225]

The "inescapable and automatic" collection of information is evidence that individuals do not voluntarily share their data with third parties.[226] A criticism of considering inescapability in the voluntariness analysis is that everything can be avoided with enough effort.[227] It can be argued that although search history records are created automatically, its production is escapable because individuals can choose to turn off the feature that allows Google to save their search history.[228] However, the collection of search history data should be deemed inescapable because it is difficult for many individuals to avoid.[229] Most individuals do not know that clearing their browser history will not clear their Google search history.[230] Many Google users have never changed their default account settings, which allows Google to collect their search history data.[231] Furthermore, individuals who use Google without an account do not have the option of disabling Google's activity tracking.[232]

---

https://www.nacdl.org/getattachment/b774a297-074f-44f4-8fea-4f7dfaa26ab3/seymour-eff-amicus-in-mts.pdf [https://perma.cc/XY2Z-JV7T] ("Keyword warrants are possible because, on the Internet, it is virtually impossible to find a website or any other information without entering search terms (also known as 'keywords') into a search engine."). *See generally* Kathleen K. Olson, *Transforming Fair Use Online: The Ninth Circuit's Productive-Use Analysis of Visual Search Engines*, 14 COMMC'N L. & POL'Y 153, 153 (2009) ("The vast amount of data available online makes search engines indispensable tools for users of the World Wide Web.").

224 *See generally Using Search Engines*, GCFGLOBAL, https://edu.gcfglobal.org/en/internetbasics/using-search-engines/1/# [https://perma.cc/BQ5A-KNNS].

225 Hazel Emnace, *23 Essential Google Search Statistics for 2022*, FIT SMALL BUS. (Oct. 25, 2022), https://fitsmallbusiness.com/google-search-statistics [https://perma.cc/82NL-F6UM].

226 *Carpenter*, 138 S. Ct. at 2223; HECHT-FELELLA, *supra* note 88, at 29.

227 Tokson, *supra* note 184, at 426–29 ("An 'inescapability' standard for Fourth Amendment protection is conceptually problematic. It cannot mean what it says. Virtually every form of digital surveillance is escapable with sufficient effort.").

228 *See id.* at 427.

229 *See id.* at 427–29 ("Few internet users actually avail themselves of these options [to prevent the disclosure of their internet data], perhaps because of concerns about cost, speed, or convenience, or because they are unaware of them.").

230 Dylan Curran, Opinion, *Browsing Porn in Incognito Mode Isn't Nearly as Private as You Think*, THE GUARDIAN (May 27, 2018, 11:33 AM), https://www.theguardian.com/commentisfree/2018/may/27/incognito-mode-what-does-it-mean-history-google-chrome-privacy-settings [https://perma.cc/Y4X3-BGL8].

231 Jason Aten, *Google Just Revealed How Many People Use Its Privacy Checkup Tool. It's Not Good News*, INC. (July 31, 2020), https://www.inc.com/jason-aten/google-just-revealed-how-many-people-use-its-privacy-checkup-tool-its-not-good-news.html [https://web.archive.org/web/20220516063114/https://www.inc.com/jason-aten/google-just-revealed-how-many-people-use-its-privacy-checkup-tool-its-not-good-news.html] ("[A]round 95 percent of people who use Google have never changed the settings that control what data the company collects and saves.").

232 *See* Declaration of Legal Investigations Support Analyst, *supra* note 6, ¶ 7.

To reiterate, the third-party doctrine should not be applied in cases involving keyword search warrants because search history data is not voluntarily shared.[233] Google does not obtain true consent from its users to collect their data; many Google users are unaware of the company's policies and practices regarding data collection.[234] Nearly everyone comes across a privacy policy at some point in their lives, but few individuals read the policy before accepting it.[235] The average privacy policy takes approximately eighteen minutes to read and requires no less than a college-level reading ability.[236] Even if they had the time and qualifications, most individuals are forced to agree if they have to use the service to participate in civic life.[237] Additionally, Fourth Amendment protections should not be abrogated merely because a user clicked "I agree" to a privacy policy when creating an account.[238] The application of the *Carpenter* test demonstrates that individuals possess a reasonable

---

233 *See In re* Search of: Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 737 n.4 (N.D. Ill. 2020) ("[M]any device users do not voluntarily relinquish information; rather, when the devices are powered on, information is sent on behalf of the individual to third parties. No voluntary action triggers this collection, and warrantless government searches conducted under the authority of the third-party doctrine should be unconstitutional." (quoting Cristina Del Rosso & Carol M. Bast, *Protecting Online Privacy in the Digital Age:* Carpenter v. United States *and the Fourth Amendment's Third-Party Doctrine*, 28 CATH. U. J.L. & TECH. 89, 121 (2020))).

234 *See* United States v. Chatrie, 590 F. Supp. 3d 901, 926 (E.D. Va. 2022) ("Even with consent, it seems clear that most Google users do not know how the consent flow to control their collection of data works . . . ."); United States v. Jones, 565 U.S. 400, 418 (2012) (Sotomayor, J., concurring) ("I for one doubt that people would accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year.").

235 Mark Sableman, *Who Reads Privacy Policies?*, THOMPSON COBURN LLP (May 31, 2017), https://www.thompsoncoburn.com/insights/blogs/internet-law-twists-turns/post/2017-05-31/who-reads-privacy-policies [https://perma.cc/UM63-X4FU]; *see* BROOKE AUXIER ET AL., PEW RSCH. CTR., AMERICANS AND PRIVACY: CONCERNED, CONFUSED AND FEELING LACK OF CONTROL OVER THEIR PERSONAL INFORMATION 37 (2019), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf [https://perma.cc/2EN3-RWJZ] ("Just 9% of adults say they always read a company's privacy policy before agreeing to the terms and conditions . . . . More than a third of adults (36%) say they never read a privacy policy before agreeing to it.").

236 Angela Chen, *Most Americans Think They're Being Constantly Tracked—And That There's Nothing They Can Do*, MIT TECH. REV. (Nov. 15, 2019), https://www.technologyreview.com/2019/11/15/238341/privacy-pew-research-data-collection-big-tech-facebook-google-apple [https://perma.cc/ZT49-5XXC].

237 *Id.*; Editorial, *How Silicon Valley Puts the 'Con' in Consent*, N.Y. TIMES (Feb. 2, 2019), https://www.nytimes.com/2019/02/02/opinion/internet-facebook-google-consent.html [https://web.archive.org/web/20230712171222/https://www.nytimes.com/2019/02/02/opinion/internet-facebook-google-consent.html] ("The clicks that pass for consent are uninformed, non-negotiated and offered in exchange for services that are often necessary for civic life.").

238 *See Chatrie*, 590 F. Supp. 3d at 936 ("[A] user simply cannot forfeit the protections of the Fourth Amendment for years of precise . . . information by selecting 'YES, I'M IN' . . . even if some text offered warning along the way.").

expectation of privacy in their search history data, necessitating a traditional search warrant.[239]

B. *Probable Cause*

The Fourth Amendment requires that search warrants be supported by probable cause, and keyword search warrants cannot meet this requirement.[240] Probable cause cannot be established because the government does not have a particular person in mind in all cases involving keyword search warrants.[241] In order to establish probable cause, there must be a fair probability that evidence of a crime will be discovered in the search.[242] Good faith is insufficient to constitute probable cause; the government official must have a reasonable belief that is supported by facts within their knowledge.[243] Probable cause can never be satisfied when it comes to keyword search warrants because the only basis for the warrant is a law enforcement official's guess that the culprit searched for a term or address that relates to the alleged crime.[244] Additionally, law enforcement officials are unable to determine whether the culprit used Google or a different search engine.[245]

Keyword search warrants are not based upon probable cause and this is clear from the keyword search warrants used in the Austin serial bombings investigation.[246] The warrants there stated that there was probable cause that the individuals who searched for the listed terms would assist law enforcement officials in identifying people who had information about the bombings.[247] The government also tried to justify its request by stating that information stored on Google's computers

---

239 *See* HECHT-FELELLA, *supra* note 88, at 29.

240 U.S. CONST. amend. IV; *see* Albert Fox Cahn & Julian Melendi, *The New Way Police Could Use Your Google Searches Against You*, SLATE (Aug. 1, 2022, 2:18 PM), https://slate.com/technology/2022/08/keyword-search-warrants-colorado-roe.html [https://perma.cc/R3X3-AJQ8].

241 Brewster, *Warrants Can Force Google*, *supra* note 5 ("[U]nlike most search warrants, keyword searches don't target a specific person or property. Instead, they could potentially hand law enforcement data on dozens, hundreds or even thousands of people unrelated to the case at hand.").

242 Illinois v. Gates, 462 U.S. 213, 238 (1983).

243 Carroll v. United States, 267 U.S. 132, 161–62 (1925) (quoting Dir. Gen. of R.R. v. Kastenbaum, 263 U.S. 25, 28 (1923)).

244 *See* Anthony W. Accurso, *New Digital Warrants Undermine Fourth Amendment*, CRIM. LEGAL NEWS (Jan. 15, 2022), https://www.criminallegalnews.org/news/2022/jan/15/new-digital-warrants-undermine-fourth-amendment [https://perma.cc/8PF9-AMBD].

245 *See id.*

246 *See* Brewster, *Exclusive*, *supra* note 14.

247 March 14 Affidavit, *supra* note 117 ¶ 6; First March 19 Affidavit, *supra* note 117 ¶ 7; Second March 19 Affidavit, *supra* note 117 ¶ 6.

"may" constitute evidence of the crimes because the information can be used to identify Google users.[248] These statements are insufficient to establish probable cause. Probable cause exists when a reasonable person would believe that a particular individual has committed a crime.[249] Probable cause does not exist when law enforcement officials apply for keyword search warrants because they are still looking for suspects.[250] Keyword search warrants should be held unconstitutional because they circumvent Fourth Amendment protections by allowing law enforcement officials to collect information about Google users without probable cause.[251]

C. *Particularity*

Probable cause must be particularized with respect to each person who is searched.[252] The Fourth Amendment requires that warrants contain a particular description of the area to be searched and the items or people to be seized.[253] Keyword search warrants are unconstitutional because they do not describe a known individual.[254] Rather, they cast a digital dragnet that can capture many innocent individuals who

---

248 First March 19 Affidavit, *supra* note 117 ¶ 14.

249 *See* Press Release, NW3C, Probable Cause, Particularity, & Demonstrating a Nexus in the Digital World (Dec. 16, 2021), https://www.nw3c.org/old-News/press-releases/article/2021/12/16/probable-cause-particularity-demonstrating-a-nexus-in-the-digital-world [https://perma.cc/L3EQ-5WQV].

250 *See* Julia Love, *Google Keyword-Search Warrants Questioned by Colorado Lawyers*, BLOOMBERG (Jan. 12, 2023, 2:31 PM), https://www.bloomberg.com/news/articles/2023-01-12/google-keyword-search-warrants-questioned-by-colorado-lawyers [https://perma.cc/L6AZ-TNBB] ("[T]he process operates in reverse—search everyone first, and identify suspects later." (quoting Petition for Rule to Show Cause ¶ 17, *In Re:* People v. Seymour, No. 2023SA12 (Colo. Jan. 11, 2023))); Motion to Suppress, *supra* note 9, ¶ 76 ("At the time, investigators simply 'didn't know' who they were looking for. . . . [They] lacked probable cause to search any one individual's search history, so instead relied on speculation and generalized suspicion to search billions." (quoting Reporter's Transcript at 84, People v. Seymour, No. 21CR20001 (Colo. Dist. Ct. Nov. 12, 2021))).

251 *See* United States v. Chatrie, 590 F. Supp. 3d 901, 929 (E.D. Va. 2022) (noting that the geofence warrant was invalid because "the warrant simply did not include any facts to establish probable cause to collect such broad and intrusive data from each one of these individuals"); *In re* Search of: Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 757 (2020) ("[I]f the government can identify [a] wrongdoer only by sifting through the identities of unknown innocent persons without probable cause and in a manner that allows officials to 'rummage where they please in order to see what turns up,' even if they have reason to believe something will turn up, a federal court in the United States of America should not permit the intrusion." (citation omitted) (quoting United States v. Sanchez-Jara, 889 F.3d 418, 421 (7th Cir. 2018))).

252 Ybarra v. Illinois, 444 U.S. 85, 91 (1979).

253 U.S. CONST. amend. IV.

254 *See* Guariglia, *supra* note 6.

happened to be searching certain terms.[255] In the Austin serial bombings investigation, the keyword search warrants required Google to include various combinations of search terms in its queries.[256] For example, one such combination was "('cardboard' OR 'package') AND ('bomb' OR 'explosive' OR 'ied' OR 'explosion' OR 'pipebomb' OR 'pipe bomb' OR 'PVC bomb')."[257] Anyone who searched for other applicable variants of the search terms would also be caught in the dragnet and have their information sent to law enforcement.[258]

The defendant in *People v. Seymour* was caught in a digital dragnet, and his motion to suppress was wrongly denied by the trial court judge.[259] The keyword search warrant in the case was not specific or narrow; it requested information about any and all Google users who searched for certain terms.[260] Contrary to the judge's assertion, it was not a targeted search because keyword search warrants do not target a specific person.[261] Instead, the warrant finds its targets among millions of users based on their internet searches.[262] Certainly, most of Google's users have not participated in the alleged crime, and their data will not be evidence of any crime at all.[263] Law enforcement officials can determine which users

---

255 Jennifer Lynch & Andrew Crocker, *EFF Files Amicus Brief in First U.S. Case Challenging Dragnet Keyword Warrant*, ELEC. FRONTIER FOUND. (June 30, 2022), https://www.eff.org/deeplinks/2022/06/eff-file-amicus-brief-first-us-case-challenging-dragnet-keyword-warrant [https://perma.cc/PFB3-Y6SJ]; Webster, *supra* note 114 ("[S]uch a wide net could catch completely routine and non-criminal searches of the victim's name by neighbors, prospective employers or business associates, journalists, or friends."); *see* Cahn & Humell, *supra* note 24 ("[K]eyword search warrants . . . upend the traditional logic of warrants and search a broad pool of innocent individuals in the hopes of finding one who is guilty."); Clayton Rice, *What Is a Keyword Search Warrant?*, CLAYTON RICE K.C. (Oct. 15, 2021), https://www.claytonrice.com/what-is-a-keyword-search-warrant [https://perma.cc/GW2H-NX2X] ("A keyword warrant authorizes the search of a crowd to find one person.").

256 March 14 Affidavit, *supra* note 117 ¶ 2; First March 19 Affidavit, *supra* note 117 ¶ 2; Second March 19 Affidavit, *supra* note 117 ¶ 2.

257 First March 19 Affidavit, *supra* note 117 ¶ 2.

258 *Id.* ("[T]his application seeks to obtain information from Google associated with the following search terms . . . or any other applicable variants of the following search queries that satisfy the below parameters in any order, inclusive of additional search terms."). Anyone in the world who searched for the relevant terms could become a suspect. *See* Affidavit in Support of an Application for a Search Warrant, *supra* note 123, ¶ 19 (noting that the incriminating searches were conducted in Georgia and the crime occurred in Florida).

259 *See* Bradbury, *supra* note 19.

260 Declaration of Legal Investigations Support Analyst, *supra* note 6, ¶ 11.

261 *See* Bradbury, *supra* note 19; Brewster, *Warrants Can Force Google*, *supra* note 5.

262 *See* Brewster, *Warrants Can Force Google*, *supra* note 5 ("A search like this, where you just have no suspects and you don't know who you're going to end up with, you really run the risk that a person is targeted based on an officer's belief that their internet search could be somehow linked to the case . . . .").

263 *See* Daniel Schwarz & Simon McCormack, *Dragnet Warrants Are Trapping Innocent People*, NYCLU (Dec. 1, 2021, 1:00 PM), https://www.nyclu.org/en/news/dragnet-warrants-are-

are relevant to their investigation, but this in itself runs afoul of the Fourth Amendment.[264] The particularity requirement acts to limit the scope of the search, and the fact that law enforcement officials have discretion in excluding data they receive from Google is evidence that the warrant is not particularized.[265]

Keyword search warrants give Google and law enforcement officials, instead of a judge, the discretion to decide which users' information will be disclosed.[266] This allows for greater intrusion into the lives and rights of law-abiding individuals.[267] Google gets to decide whether the government has adequately narrowed its requests.[268] If the warrant allows for it, law enforcement officials can seek additional information about any accounts they decide are relevant without having to obtain an additional warrant.[269] Without judicial approval or objective criteria to narrow the list of users, law enforcement officials have unfettered discretion to obtain the personal information of many individuals.[270]

---

trapping-innocent-people [https://perma.cc/7LL8-3TVL]. Keyword search warrants "can place hundreds or thousands of unsuspecting and innocent people in the crosshairs of law enforcement, threatening their rights to be free from unreasonable government searches." *Id.*; JEFF KOSSEFF, THE UNITED STATES OF ANONYMOUS: HOW THE FIRST AMENDMENT SHAPED ONLINE SPEECH 162 (2022) ("[K]eyword [search] warrants and geofence warrants . . . run the risk of identifying innocent people and linking them with high-profile crimes merely because they had the bad fortune to search for the wrong term or be physically located near a crime.").

264 Declaration of Legal Investigations Support Analyst, *supra* note 6, ¶ 8; *see* United States v. George, 975 F.2d 72, 76 (2d Cir. 1992) ("Absent some limitation curtailing the officers' discretion when executing the warrant, the safeguard of having a magistrate determine the scope of the search is lost.").

265 *Particularity*, JUSTIA, https://law.justia.com/constitution/us/amendment-04/09-particularity.html [https://perma.cc/CN9N-KCMT]; *see* Marron v. United States, 275 U.S. 192, 196 (1927) ("The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant."); Stanford v. Texas, 379 U.S. 476, 481–85 (1965).

266 *See* United States v. Chatrie, 590 F. Supp. 3d 901, 933 (E.D. Va. 2022).

267 *See* Cushing, *supra* note 206.

268 *See* Cullen Seltzer, *Google Knows Where You've Been. Should It Tell the Police?*, SLATE (May 16, 2022, 11:04 AM), https://slate.com/technology/2022/05/google-geofence-warrants-chatrie-location-tracking.html [https://perma.cc/3RJA-DA69]; Declaration of Legal Investigations Support Analyst, *supra* note 6, ¶ 10.

269 Declaration of Legal Investigations Support Analyst, *supra* note 6, ¶ 9.

270 *See, e.g.*, *Chatrie*, 590 F. Supp. 3d at 934 ("[T]he warrant provided law enforcement unchecked discretion to seize more intrusive and personal data with each round of requests—without ever needing to return to a neutral and detached magistrate for approval."); Lynch, *supra* note 152 (noting that one court held a geofence warrant to have "violated the Fourth Amendment because it failed to require police to come back to the court for a new warrant at each step of the process, instead providing officers with unbridled discretion to determine who to target for further investigation"). The keyword search warrants in the Austin serial bombings investigation did not contain language preventing law enforcement officials from deciding which accounts and how many of them they could seek identifying information from. *See* sources cited *supra* note 117.

Particularity was constitutionalized to prevent this kind of warrant from existing.[271]

In *Ybarra v. Illinois*, the Court stated that searching everyone in the tavern was unconstitutional because there was no probable cause to believe that any person in the bar other than the bartender was violating the law.[272] Probable cause did not exist at the time the warrant was issued nor at the time it was executed.[273] The police did not know anything about Ybarra when they walked into the tavern and had no reason to believe that he was associated with any crime.[274] The search warrant had only described the place and the bartender; no one else was mentioned.[275] Keyword search warrants are unable to identify even one individual.[276] The mere possibility that the perpetrator searched for a term or address related to the crime before it occurred does not establish probable cause to search through all users' data.[277] Law enforcement officials have no reason to believe that every responsive user has the information they are seeking.[278] Search warrants must be specific and particularized to each person that the law enforcement official wishes to search.[279] This is not possible in situations involving keyword search warrants because law enforcement officials are using the warrants to find suspects.[280]

D. *Application of* Chatrie *to Keyword Search Warrants*

Law enforcement officials also use geofence warrants to find suspects, and since geofence warrants were ruled unconstitutional in *Chatrie*, keyword search warrants should be declared unconstitutional as well.[281] Keyword search warrants are far more invasive than geofence warrants because the searches are not limited by location and because the

---

271 Note, *supra* note 200, at 2518 ("Particularity was constitutionalized in response to these 'reviled general warrants.' Since then, it has generally been understood that no warrant can authorize the search of everything or everyone in sight." (footnote omitted) (quoting Riley v. California, 573 U.S. 373, 403 (2014))); Maryland v. Garrison, 480 U.S. 79, 84 (1987) ("The manifest purpose of this particularity requirement was to prevent general searches.").

272 444 U.S. 85, 90 (1979).

273 *Id.*

274 *Id.* at 90–91.

275 *Id.* at 88.

276 *See* Cushing, *supra* note 206.

277 *See Ybarra*, 444 U.S. at 91.

278 *See* Gilens, Lynch & Alimonti, *supra* note 23.

279 *Ybarra*, 444 U.S. at 91.

280 Schuppe, *supra* note 1.

281 *See* United States v. Chatrie, 590 F. Supp. 3d 901, 941 (E.D. Va. 2022).

requested time period could be much longer.[282] Law enforcement officials could seek months of information from Google with a keyword search warrant, which is vastly different than the one-hour time frame stated in the geofence warrant in *Chatrie*.[283] Since the length of time is greater, more users are likely to be affected by keyword search warrants.[284] Law enforcement officials attempt to justify reverse search warrants by stating that these warrants can aid their investigation by identifying suspects or witnesses.[285] This reasoning is weaker when applied to keyword search warrants because it is possible that someone who was caught in a geofence may have witnessed the crime, but it is unlikely that a witness would have searched for the incriminating keywords.[286]

The court in *Chatrie* held the geofence warrant to be unconstitutional because it lacked particularized probable cause as to every user in the geofence.[287] Keyword search warrants should be held unconstitutional because they suffer from the same defect; law enforcement officials cannot justify the collection of personal information of everyone who searched for certain keywords.[288] The detective in *Chatrie* believed that the geofence warrant would identify the perpetrator because the surveillance footage showed him using an Android cell phone, and most Android cell phones have an associated Google account.[289] Despite this, the court held that the footage did not justify such a broad warrant.[290] It is more difficult to defend the use of keyword search warrants because many different individuals can search for the same terms or addresses.[291] Additionally, the perpetrator may not

---

282 *See* Bhuiyan, *supra* note 8 ("[K]eyword search warrants are not necessarily geographically or tangibly tied to a specific crime and could make suspects out of people around the world who happened to search for specific terms.").

283 *See, e.g.*, First March 19 Affidavit, *supra* note 117 ¶ 6 (seeking approximately two months' worth of information); *see also Chatrie*, 590 F. Supp. 3d at 914.

284 Bhuiyan, *supra* note 8 (explaining that keyword search warrants are "potentially more far-reaching than geofence warrants").

285 *Chatrie*, 590 F. Supp. 3d at 929; *see* March 14 Affidavit, *supra* note 117 ¶ 28; First March 19 Affidavit, *supra* note 117 ¶ 32; Second March 19 Affidavit, *supra* note 117 ¶ 29.

286 *See* Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html [https://archive.ph/at9li].

287 *Chatrie*, 590 F. Supp. 3d at 927.

288 *See* Gilens, Lynch & Alimonti, *supra* note 23.

289 *Chatrie*, 590 F. Supp. 3d at 920.

290 *Id.* at 930.

291 Memorandum from Diane Akerman, Staff Att'y, The Legal Aid Soc'ys Digit. Forensics Unit, to N.Y. State Legislature 2 (Jan. 3, 2022), https://www.nyclu.org/sites/default/files/220201-memo-legalaidreversewarrant.pdf [https://perma.cc/Q8JQ-NBCT] (explaining that the use of keyword search warrants "amounts to a nationwide violation of people's rights" because "individuals may

have searched up any terms or addresses relating to the crime.[292] Keyword search warrants inevitably and unjustly collect data from private citizens who are not associated with any crime at all.[293] Some individuals may even be wrongly accused of a crime as a result of using such a warrant.[294] Traditional search warrants minimize this risk and protect individual privacy interests against government intrusion by requiring probable cause and particularity.[295]

The *Chatrie* court did not address whether obtaining location history information constituted a search under the Fourth Amendment, but it is clearly a search in the context of search history information.[296] The third-party doctrine can arguably be applied to location history information because opting into Google's location history service is voluntary and is not required to participate in modern society.[297] Unlike location history, search history is collected by Google without users having to opt in to the service.[298] Since search history is saved by default, it cannot be said that users voluntarily turn over their information to

---

have searched a term that law enforcement has deemed relevant to their investigation, regardless of how broad or common the term may be").

292 *See* Gilens, Lynch & Alimonti, *supra* note 23 ("Keyword warrants allow the police to learn anyone and everyone who may have searched for particular terms on the off-chance one of those people could have been involved with the crime.").

293 *See Chatrie*, 590 F. Supp. 3d at 930.

294 *See* Jon Schuppe, *Google Tracked His Bike Ride past a Burglarized Home. That Made Him a Suspect.*, NBC NEWS (Mar. 7, 2020, 6:22 AM), https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761 [https://perma.cc/2N3E-3NUA] (describing how a Google user had to spend thousands of dollars for a lawyer after the results of a geofence warrant wrongfully made him a suspect in a burglary investigation). There have also been concerns that pregnant individuals can be prosecuted for searching for abortion providers. Bobby Allyn, *Privacy Advocates Fear Google Will Be Used to Prosecute Abortion Seekers*, NPR (July 11, 2022, 5:00 AM) https://www.npr.org/2022/07/11/1110391316/google-data-abortion-prosecutions [https://perma.cc/2MMB-EZ78].

295 *See* Cassandra Zietlow, *Reverse Location Search Warrants: Law Enforcement's Transition to 'Big Brother'*, 23 N.C. J.L. & TECH. 669, 674–75 (2022).

296 *See Chatrie*, 590 F. Supp. 3d at 930; Orin S. Kerr, *The Fourth Amendment and Geofence Warrants: A Critical Look at* United States v. Chatrie, VOLOKH CONSPIRACY (Mar. 11, 2022, 4:38 PM), https://reason.com/volokh/2022/03/11/the-fourth-amendment-and-geofence-warrants-a-critical-look-at-united-states-v-chatrie [https://perma.cc/Q2NW-ZHJZ].

297 *See* Kerr, *supra* note 296.

298 Matt G. Southern, *User Search History as a Google Ranking Factor: What You Need to Know*, SEARCH ENGINE J. (Mar. 7, 2022), https://www.searchenginejournal.com/ranking-factors/user-search-history [https://perma.cc/Y8A7-KLA3]; Russell Brandom, *Google Will Now Auto-Delete Location and Search History by Default for New Users*, THE VERGE (June 24, 2020, 12:00 PM), https://www.theverge.com/2020/6/24/21301718/google-auto-delete-location-search-history-default-myactivity [https://perma.cc/V7GY-NAR7] ("Google will set web and app searches to auto-delete after 18 months even if users take no action at all. Google's location history is off by default . . . .").

Google.[299] Additionally, using Google is required to participate in modern society.[300] Therefore, keyword search warrants should be deemed unconstitutional, as geofence warrants have been, due to their disregard for individual privacy rights and invasive nature.[301]

E. *The Lack of Necessity for Keyword Search Warrants*

Keyword search warrants should never be issued because there are less invasive methods that law enforcement officials can use to identify a suspect without infringing on the constitutional rights of blameless individuals.[302] Keyword search warrants violate the Fourth Amendment's prohibition on unreasonable searches because they are unnecessary in identifying perpetrators.[303] In the Austin serial bombings investigation, the police were able to find Conditt through traditional investigative techniques.[304] They had realized that the bombs shared many similarities, including that they were all made from common household ingredients.[305] Investigators went to stores all over Austin to find out if any suspicious purchases had been made.[306] They checked receipts and sales records, which became critical evidence against Conditt.[307] Additionally, Conditt was seen on security video at a FedEx store shipping an explosive device and at a Home Depot buying supplies for the bombs.[308] Both videos showed a red 2002 Ford Ranger, which provided law enforcement officials with his license plate number.[309] After comparing the name on a receipt and a photo of the individual from

---

299 *See Chatrie*, 590 F. Supp. 3d at 935. Even if users had to enable search history, it would not show that users accepted the accompanying risks of disclosing everything they had ever searched. *See id.* at 936.

300 *See supra* Section II.A.5.

301 *See* Schwarz & McCormack, *supra* note 263; Press Release, ACLU, ACLU Argues Evidence from Privacy-Invasive Geofence Warrants Should Be Suppressed (Jan. 30, 2023, 8:00 AM), https://www.aclu.org/press-releases/aclu-argues-evidence-from-privacy-invasive-geofence-warrants-should-be-suppressed [https://perma.cc/D2LC-3Q8F].

302 *See* Rice, *supra* note 255.

303 *See id.*; Doug Criss, *Police Used Store Receipts and Internet Searches to Identify Austin Bombing Suspect*, CNN, https://www.cnn.com/2018/03/21/us/austin-bomber-narrative-trnd [https://perma.cc/4AM3-47GC] (Mar. 22, 2018, 1:42 AM).

304 Rice, *supra* note 255.

305 Criss, *supra* note 303; First March 19 Affidavit, *supra* note 117, ¶ 30.

306 Criss, *supra* note 303.

307 *Id.*

308 *Inside the FBI's Race to Stop Austin, Texas*, *supra* note 115.

309 Abby Johnston, *Who Was Mark Conditt? Here's What We Know About the Austin Bombing Suspect*, TEX. MONTHLY (Mar. 22, 2018), https://www.texasmonthly.com/news-politics/mark-conditt-heres-know-austin-bombings-suspect [https://perma.cc/J88A-KWYM].

Home Depot's security video with Conditt's driver's license, it was clear that the law enforcement officials had identified the bomber.[310] The Austin serial bombings investigation illustrates that traditional investigative methods, which respect constitutional rights and prioritize individual privacy, can lead to the successful identification of suspects, rendering keyword search warrants unnecessary.[311]

CONCLUSION

When presented with the issue, state and federal courts should establish that keyword search warrants are unconstitutional because they violate the Fourth Amendment to the United States Constitution. The application of the *Carpenter* test to search history data shows that individuals have a reasonable expectation of privacy in their data. Therefore, a search occurs when law enforcement officials attempt to obtain this information. Keyword search warrants cannot be substituted for traditional search warrants because they do not meet the Fourth Amendment requirements of probable cause and particularity. The government does not have a suspect in mind when it requests keyword search warrants.[312] These warrants provide law enforcement officials with broad discretion to search and seize data about anyone who searched for certain terms or addresses.[313] They are the modern-day digital equivalent of a general warrant.[314] Courts must refuse to approve these warrants because they are overbroad and have the potential to implicate many innocent individuals.[315] Keyword search warrants allow for surveillance that was not possible in the past.[316] They are unnecessary because the government can find perpetrators using traditional investigative methods.[317] Several courts in the United States have held geofence warrants to be unconstitutional, and others should follow their example in situations involving keyword search warrants.[318] Technology is advancing at a rapid pace, and the law must progress with it.

---

310 *Inside the FBI's Race to Stop Austin, Texas, Bombing Spree*, *supra* note 115.

311 *See id.*

312 *See* Brewster, *Warrants Can Force Google*, *supra* note 5.

313 *See* Declaration of Legal Investigations Support Analyst, *supra* note 6, ¶¶ 11–13.

314 *See* Gilens, Lynch & Alimonti, *supra* note 23.

315 *See id.*

316 *See* HECHT-FELELLA, *supra* note 88, at 10.

317 *See Inside the FBI's Race to Stop Austin, Texas, Bombing Spree*, *supra* note 115.

318 *See* sources cited *supra* note 152.