

WHEN QUERIES BECOME CLUES: KEYWORD SEARCH WARRANTS AND THE MODERN FOURTH AMENDMENT

*Rory Owens**

INTRODUCTION

On a summer evening in 2016, a man broke into a Pennsylvania woman's home, forced her into a waiting vehicle, and committed a brutal assault in a remote camper before abandoning her in a cornfield.¹ With limited physical evidence and few immediate leads, investigators turned to an unconventional tactic: They obtained a keyword search warrant directing Google to disclose the IP addresses of any users who had recently searched for the victim's address.² Google complied, returning an IP address that ultimately led law enforcement to John Edward Kurtz.³ This one digital breadcrumb provided the key to solving the crime—and highlighted a powerful but controversial new law enforcement tool.

Keyword search warrants represent a novel extension of government surveillance in the digital age. Rather than requiring a search engine to disclose records tied to a known individual, these warrants compel providers to scan their entire corpus of user queries for a single term—such as a crime scene address or victim's name—and then produce the subset of searches that match.⁴ While keyword search warrants share some similarities with the more widely scrutinized geofence warrant,⁵ much of the attention in courts and scholarship has focused on the latter,⁶ leaving the unique constitutional

* J.D. Candidate, Notre Dame Law School, 2026. I am grateful to Dennis Wieboldt and John Gatt for their feedback, as well as to my colleagues on the *Notre Dame Law Review* for their careful edits.

1 *Commonwealth v. Kurtz*, 294 A.3d 509, 516–17 (Pa. Super. Ct. 2023).

2 *Id.* at 517.

3 *Id.*

4 *See infra* Section II.A.

5 Both keyword search warrants and geofence warrants are examples of reverse search warrants. Rather than targeting data tied to a known suspect, reverse search warrants compel the provider to disclose information on *every* user who meets certain criteria to identify suspects. *See Note, Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2509 (2021).

6 *See, e.g., United States v. Smith*, 110 F.4th 817 (5th Cir. 2024); *United States v. Chattrie*, 136 F.4th 100 (4th Cir. 2025) (en banc) (per curiam); *Note, supra* note 5; Haley Amster & Brett

contours of keyword search warrants comparatively unexamined. Critics maintain that keyword search warrants risk sweeping in countless unwitting users and strain the Fourth Amendment's twin requirements of probable cause and particularity.⁷ Yet as the *Kurtz* investigation illustrates, keyword search warrants can be narrowly crafted and extremely effective when used for a crime with specific digital clues. Further, whether accessing this trove of query data constitutes a Fourth Amendment "search" at all remains an open and critical question.⁸

This Note addresses the constitutional questions that keyword search warrants have created in light of modern Fourth Amendment jurisprudence.⁹ Part I provides an overview of current Fourth Amendment doctrine, outlining the modern privacy-based framework, the third-party doctrine, *Carpenter v. United States*, and the core requirements of probable cause and particularity. Part II introduces keyword search warrants as a new form of reverse search warrant. It defines how they operate and highlights two recent state court cases that address their constitutionality. Part III offers a constitutional analysis of keyword search warrants. Section III.A argues that obtaining a user's query data—even if partially de-identified—constitutes a "search" under *Carpenter*, given how extensively it can reveal an individual's private life. Section III.B contends that keyword search warrants are not per se invalid: when tailored to specific times, locations, and search terms, they can satisfy both probable cause and particularity.

Diehl, Note, *Against Geofences*, 74 STAN. L. REV. 385 (2022); Brian L. Owsley, *The Best Offense is a Good Defense: Fourth Amendment Implications of Geofence Warrants*, 50 HOFSTRA L. REV. 829 (2022).

7 See, e.g., Nicole Chan, Note, *Wrong Search at the Wrong Time: Keyword Search Warrants and the Fourth Amendment*, 45 CARDOZO L. REV. 271 (2023); Chelsa Camille Edano, Comment, *Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants*, 97 WASH. L. REV. 977 (2022).

8 See, e.g., Helen Winters, Note, *An (Un)reasonable Expectation of Privacy? Analysis of the Fourth Amendment When Applied to Keyword Search Warrants*, 107 MINN. L. REV. 1369, 1389–1408 (2023).

9 This Note analyzes keyword search warrants within the Supreme Court's existing Fourth Amendment jurisprudence. The focus is descriptive rather than prescriptive; it seeks to explain how these warrants are evaluated under current doctrine, not to advance an independent theory of Fourth Amendment meaning.

I. MODERN FOURTH AMENDMENT DOCTRINE

A. *The Reasonable Expectation of Privacy*

To protect individual privacy and security against arbitrary government intrusions, the Fourth Amendment ensures “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.”¹⁰ It was drafted as a “response to the reviled ‘general warrants’ and ‘writs of assistance’ of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.”¹¹

For nearly two centuries, the prevailing understanding of the Fourth Amendment was anchored in the common law conception of property as the primary subject of constitutional safeguards.¹² However, a shift away from this property-based approach began in 1928 in *Olmstead v. United States*, where the Court held that the wiretapping of the defendant’s home did not violate the Fourth Amendment because “[t]he evidence was secured by the use of the sense of hearing and that only.”¹³ Since “[t]here was no entry of the houses or offices of the defendants,” and thus no physical trespass, there was a limit to what could be constitutionally protected.¹⁴ It was Justice Brandeis’s dissent, however, that sowed the seeds of a doctrinal shift. Rejecting the necessity of physical trespass, Brandeis argued that “every unjustifiable intrusion by the Government upon the *privacy* of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.”¹⁵ Thus, in Brandeis’s view, privacy—not property—was what mattered.

Justice Brandeis’s broader, privacy-oriented approach to the Fourth Amendment was formally vindicated nearly forty years later when, in 1967, the Court decided *Katz v. United States*.¹⁶ There, the Court famously articulated that “the Fourth Amendment protects people, not places.”¹⁷ Thus, the critical inquiry was no longer tethered to whether the government trespassed upon a particular enclosure.¹⁸ Instead, the Court understood that

10 *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018) (alteration in original) (quoting U.S. CONST. amend. IV); *see also* *Camara v. Mun. Ct.*, 387 U.S. 523, 528 (1967).

11 *Carpenter*, 138 S. Ct. at 2213 (quoting *Riley v. California*, 573 U.S. 373, 403 (2014)).

12 *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 816 (2004).

13 *Olmstead v. United States*, 277 U.S. 438, 464 (1928), *overruled by* *Katz v. United States*, 389 U.S. 347 (1967), and *Berger v. New York*, 388 U.S. 41 (1967).

14 *Id.*

15 *Id.* at 478 (Brandeis, J., dissenting) (emphasis added).

16 *Katz*, 389 U.S. 347.

17 *Id.* at 351.

18 *Id.* at 353.

constitutional safeguards of the Fourth Amendment must turn on whether the government's conduct interferes with an individual's privacy interests.¹⁹

While Justice Brandeis's *Olmstead* dissent articulated the privacy-based theory underlying *Katz*, Justice Harlan's now-iconic concurrence supplied its doctrinal framework. Justice Harlan posited a two-step test: First, a person must have exhibited an actual, subjective expectation of privacy; second, this expectation must be "one that society is prepared to recognize as 'reasonable.'"²⁰ Although originally articulated in a concurrence, this formulation swiftly evolved into the dominant mode of Fourth Amendment analysis.²¹ Today, it is this "reasonable expectation of privacy"²² standard that guides inquiries into whether a government action constitutes a search and thereby triggers constitutional protections.

B. The Third-Party Doctrine

During the mid-twentieth century, even before the Court fully embraced a privacy-focused view of the Fourth Amendment, another concept in Fourth Amendment jurisprudence was taking shape: the third-party doctrine. Through a series of cases, the Court began to recognize that when a person shares information with someone else—a "third party"—that individual's privacy interests may be reduced, and the Fourth Amendment might not provide the same level of protection.

The third-party doctrine originated in cases involving undercover agents.²³ In its 1952 decision in *On Lee v. United States*, the Court held that a defendant had no Fourth Amendment claim when his friend, acting as a government informant, secretly recorded the defendant's incriminating statements.²⁴ By speaking to someone who might later reveal the statements, the defendant assumed the risk of disclosure.²⁵ The Court, in 1971, reaffirmed this principle post-*Katz* in *United States v. White*, holding that a defendant likewise assumed the risk of disclosure when confiding in a wired informant.²⁶

The second line of third-party doctrine cases involved third-party business records.²⁷ In *United States v. Miller*, decided in 1976, the Court held that bank records were not protected by the Fourth Amendment because they would be used in the ordinary course of business and were voluntarily shared

19 See *id.* at 359.

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

21 See, e.g., *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018).

22 See, e.g., *id.* at 2219.

23 See Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 567–69 (2009).

24 *On Lee v. United States*, 343 U.S. 747, 749–54 (1952).

25 See *id.* at 753–54.

26 *United States v. White*, 401 U.S. 745, 752 (1971).

27 See Kerr, *supra* note 23, at 569–70.

with the bank²⁸—a rationale that was also applied in *Couch v. United States*²⁹ in 1973 and later in *United States v. Payner* in 1980.³⁰

The development of the third-party doctrine culminated in the Court's 1980 decision *Smith v. Maryland*.³¹ There, the Court held that using a pen register to record numbers dialed on a home phone was not a Fourth Amendment search because the "petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business."³² Thus, information voluntarily shared with third parties falls outside the Fourth Amendment's protections.

C. *Carpenter and the Fourth Amendment in the Digital Age*

For nearly half a century, the *Katz* reasonable-expectation-of-privacy test and the third-party doctrine defined the boundaries of Fourth Amendment protections. Yet both frameworks have faced significant criticism. Scholars and courts alike have faulted the *Katz* standard for its unpredictability and difficulty of application.³³ The third-party doctrine has likewise come under fire for failing to safeguard privacy in an era of routine information sharing.³⁴ It was perhaps inevitable, then, that as law enforcement embraced new surveillance technologies, the doctrinal framework for defining what constitutes a Fourth Amendment search would encounter renewed pressures. These pressures came to a head with the Court's 2018 decision in *Carpenter v. United States*.³⁵

28 *United States v. Miller*, 425 U.S. 435, 442–43 (1976), *superseded by statute*, Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3641.

29 *Couch v. United States*, 409 U.S. 322, 335 (1973) ("[T]here can be little expectation of privacy where records are handed to an accountant, knowing that mandatory disclosure of much of the information therein is required in an income tax return.").

30 *United States v. Payner*, 447 U.S. 727, 732 (1980) (holding that an individual has no expectation of privacy "in copies of checks and deposit slips retained by his bank").

31 *Smith v. Maryland*, 442 U.S. 735 (1979).

32 *Id.* at 744.

33 See *Minnesota v. Carter*, 525 U.S. 83, 97 (1998) (Scalia, J., concurring); Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1511 (2010); Orin S. Kerr, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 115 (2015); Matthew Tokson, *The Carpenter Test as a Transformation of Fourth Amendment Law*, 2023 U. ILL. L. REV. 507, 512–15; Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 385–88 (1974); William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1824–25 (2016).

34 See Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 113 (2008); Steven M. Bellovin, Matt Blaze, Susan Landau & Stephanie K. Pell, *It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law*, 30 HARV. J.L. & TECH. 1, 22–31 (2016); Mary Graw Leary, *Katz on a Hot Tin Roof—Saving the Fourth Amendment from Commercial Conditioning by Reviving Voluntariness in Disclosures to Third Parties*, 50 AM. CRIM. L. REV. 341, 379 (2013); Tokson, *supra* note 33, at 515–16.

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

In *Carpenter*, the government, without a warrant supported by probable cause, requested and received cell-site location information (CSLI) from the defendant's wireless cell carrier.³⁶ CSLI consists of time-stamped records created each time a cell phone connects to a nearby cell site, allowing wireless carriers to track the phone's location with increasing precision as the density of cell sites grows.³⁷ Wireless providers collect and store this data for various business purposes, and as modern phones generate CSLI more frequently—from calls, texts, and routine data connections—its volume and accuracy continue to expand.³⁸ The CSLI, composed of nearly 13,000 location points of the defendant over several days, allowed the government to produce maps that placed the defendant's phone near four robberies.³⁹

The Court acknowledged first that the longer-term monitoring of an individual's whole movements impinges upon their reasonable expectation of privacy.⁴⁰ It likened CSLI to GPS tracking, describing it as “detailed, encyclopedic, and effortlessly compiled.”⁴¹ Granting law enforcement unrestricted access to such data runs counter to any expectation that authorities would refrain from “secretly monitor[ing] and catalog[ing] every single movement of an individual[]” for an extended period of time.⁴² This location information can expose not only where a person travels but also sensitive matters related to one's “familial, political, professional, religious, and sexual associations.”⁴³ Moreover, officers need not identify a particular individual to track in advance, nor determine when to begin monitoring.⁴⁴

At the same time, the Court acknowledged that the third-party doctrine was implicated, but cautioned that applying it to CSLI would “fail[] to contend with the seismic shifts in digital technology.”⁴⁵ Although individuals may have a diminished expectation of privacy in information voluntarily conveyed to others, the Court emphasized that this “does not mean that the Fourth Amendment falls out of the picture entirely.”⁴⁶ The Court reiterated the two primary rationales underlying the third-party doctrine: the nature of the information sought and the voluntariness of exposure of that information

36 *Id.* at 2212–13.

37 *Id.* at 2211–12.

38 *Id.* at 2212.

39 *Id.* at 2212–13.

40 *Id.* at 2215; *see also* *United States v. Jones*, 565 U.S. 400, 430 (2012) (Alito, J., concurring) (“[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.”).

41 *Carpenter*, 138 S. Ct. at 2216.

42 *Id.* at 2217 (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring in judgment)).

43 *Id.* (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).

44 *See id.* at 2218.

45 *Id.* at 2219 (“Unlike the nosy neighbor who keeps an eye on comings and goings, [cell phone carriers] are ever alert, and their memory is nearly infallible.”).

46 *Riley v. California*, 573 U.S. 373, 392 (2014).

to third parties.⁴⁷ It then reasoned that applying the third-party doctrine to CSLI would go against these rationales.⁴⁸ Unlike the relatively limited data in *Smith* and *Miller*, CSLI compiles “a detailed chronicle of a person’s physical presence” across an expansive time frame—“every day, every moment, over several years.”⁴⁹ Moreover, the Court stressed that CSLI is not “shared” in a traditional sense: Cell phones have become “‘such a pervasive and insistent part of daily life’ that carrying one is indispensable to participation in modern society,” and CSLI is collected automatically without any affirmative conduct by the user.⁵⁰ Thus, the individual is not assuming the risk of relinquishing these comprehensive location details to a third party.

The Court declined to announce a bright-line rule for when the Fourth Amendment’s protections attach. Instead, it identified several characteristics of CSLI that supported recognizing a cognizable privacy interest exempt from the third-party doctrine: its “deeply revealing nature,” its “depth, breadth, and comprehensive reach,” and the “inescapable and automatic nature of its collection.”⁵¹ Although the Court framed *Carpenter*’s holding as narrow,⁵² lower courts have relied on some or all of these same characteristics to conclude that the third-party doctrine does not apply to other types of information.⁵³ Accordingly, these characteristics are instructive in

47 See *Carpenter*, 138 S. Ct. at 2219–20.

48 See *id.*

49 *Id.* at 2220.

50 *Id.* (quoting *Riley*, 573 U.S. at 385).

51 *Id.* at 2223.

52 *Id.* at 2220 (“We do not express a view on matters not before us: real-time CSLI or ‘tower dumps’ (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras.”).

53 See Matthew Tokson, *The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018–2021*, 135 HARV. L. REV. 1790, 1821 (2022) (“There were 217 decisions that reached a determinative, yes-or-no ruling on a Fourth Amendment search under *Carpenter*. Of these, 129 decisions mentioned at least one of the *Carpenter* factors in reaching a judgment.”). I use the term “characteristics” rather than “factors” because the legal landscape following *Carpenter* remains unsettled regarding whether the Court in fact announced a new, multi-factor test—and, if so, what its precise contours might be. Although many scholars believe *Carpenter* inaugurated a factor-based approach, they disagree sharply on which considerations matter and how they should be weighed. See, e.g., Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. 357, 369–70 (2019); Susan Freiwald & Stephen Wm. Smith, *The Carpenter Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 219 (2018); Tokson, *supra*, at 1830; Winters, *supra* note 8, at 1390; Luiza M. Leão, Note, *A Unified Theory of Knowing Exposure: Reconciling Katz and Carpenter*, 97 N.Y.U. L. REV. 1669, 1684 (2022). At the same time, some courts maintain that *Carpenter* did not meaningfully alter the doctrinal framework and instead merely applied settled principles to a novel technological context. See, e.g., *United States v. Chatrie*, 107 F.4th 319, 333–34 (4th Cir. 2024) (“Contrary to [claims that *Carpenter* promulgated a factor-based balancing test], however, *Carpenter* did not cast away the decisions that preceded it.” *Id.* at 333), *aff’d en banc*, 136 F.4th 100 (4th Cir. 2025); *United States v. Davis*, 109 F.4th 1320, 1328–31 (11th Cir. 2024) (declining to mention any of the *Carpenter* “factors” in analyzing whether there was a Fourth Amendment privacy interest in Google location data). This Note does not engage in a multi-factor

determining whether certain forms of information requested by law enforcement are constitutionally protected.

Where do things now stand? Before *Carpenter*, government action qualified as a Fourth Amendment search only when it violated a person's reasonable expectation of privacy. Under the third-party doctrine, a person's reasonable expectation of privacy in information voluntarily shared with others is substantially diminished and, in some circumstances, eliminated altogether. In *Carpenter*, however, the Court carved out a narrow exception to the third-party doctrine for CSLI because it possesses distinctive characteristics that set it apart from other types of information. Although the scope of this exception remains unsettled, Section III.A contends that keyword search data should fall within it.

D. Probable Cause and Particularity

Once conduct is deemed a Fourth Amendment "search," a warrant is typically required. That warrant must satisfy two core requirements: it must be supported by probable cause and be particularized as to the place to be searched and the items to be seized.⁵⁴

Probable cause is a "flexible, common-sense standard."⁵⁵ Under the totality of the circumstances, it exists when there is a "fair probability" that evidence of a crime will be found in a particular location.⁵⁶ It does not require proving that law enforcement's belief is correct or even "more likely true than false."⁵⁷ Rather, it calls for facts that "warrant a man of reasonable caution in the belief" that a location may contain contraband, stolen property, or evidence of a crime.⁵⁸

Probable cause must also be particularized.⁵⁹ And where heightened privacy interests are implicated, a stricter particularity requirement applies.⁶⁰ First, the place to be searched must be particular. In *Wong Sun v. United States*, for instance, the Court found that there was no probable cause to search thirty blocks merely to locate a single laundromat allegedly selling heroin, as such an expansive search invited law enforcement to search the entire area to turn up evidence of any crime "whether by chance or other

balancing test but instead contends that keyword search data shares each of the "characteristics" of CSLI described in *Carpenter*, albeit with some overlapping more closely than others. Accordingly, this Note maintains that there is a reasonable expectation of privacy in keyword search data and the third-party doctrine should similarly not apply.

54 U.S. CONST. amend. IV.

55 *Texas v. Brown*, 460 U.S. 730, 742 (1983).

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

57 *Texas*, 460 U.S. at 742.

58 *Carroll v. United States*, 267 U.S. 132, 162 (1925).

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

60 Note, *supra* note 5, at 2526.

means.”⁶¹ Yet the warrant need not identify an exact location with perfect precision.⁶² In *United States v. Karo*, the Court held that while warrantless installation of a beeper tracker on a container in a moving car did not violate the Fourth Amendment, a warrant was required to monitor the device once it entered a private residence.⁶³ The Court rejected the government’s argument that the particularity requirement is impracticable for beepers because their location changes over time and the residence ultimately entered cannot be identified in advance.⁶⁴ Instead, the Court clarified that the particularity requirement would be satisfied by describing “the object into which the beeper is to be placed, the circumstances that led agents to wish to install the beeper, and the length of time for which beeper surveillance is requested.”⁶⁵

Second, the warrant must be particular as to the items to be seized. This requirement “makes general searches under [a constitutionally valid warrant] impossible.”⁶⁶ The warrant should be drawn so that “nothing is left to the discretion of the officer executing the warrant,”⁶⁷ but it need not detail the exact objects. In *Steele v. United States*, the Court held that describing “cases of whiskey” was sufficiently particular—even without specifying the exact cases law enforcement had observed being delivered.⁶⁸

II. THE EMERGENCE OF KEYWORD SEARCH WARRANTS

A. What is a Keyword Search Warrant?

A keyword search warrant (sometimes called a “reverse keyword warrant”) is used by law enforcement to compel a search engine company to disclose the identities of anyone who may have searched for a particular “keyword.”⁶⁹ Search engine companies are able to provide law enforcement with the information they request because these search engines retain detailed personal data about search users. For example, Google can collect, if provided: a person’s name, phone number, address, demographic information, commercial information, biometric information, internet and network information, geolocation data, voice information, professional

61 *Wong Sun v. United States*, 371 U.S. 471, 480–81 (1963).

62 *United States v. Ross*, 456 U.S. 798, 821 (1982) (“[A] warrant that authorizes an officer to search a home for illegal weapons also provides authority to open closets, chests, drawers, and containers in which the weapon might be found.”).

63 *United States v. Karo*, 468 U.S. 705 (1984).

64 *Id.* at 718.

65 *Id.*

66 *Marron v. United States*, 275 U.S. 192, 196 (1927).

67 *Id.*

68 *Steele v. United States*, 267 U.S. 498, 504 (1925).

69 See 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/FL7U-WNHF].

information, educational information, photos, videos, emails and documents.⁷⁰ Often, law enforcement is looking for whether a person searched for “a victim’s name or a particular address where a crime has occurred.”⁷¹ In doing so, law enforcement is able to create a list of potential suspects in the crime.⁷²

Little is known about how often keyword search warrants are used and the procedures that law enforcement employs to obtain data from search engine companies.⁷³ However, Google has recently expanded on how it processes law enforcement requests for its search engine data.⁷⁴ Google’s Legal Investigations Support (LIS) team first “creates a text-based query (that can include letters, numbers, or characters) based on the requirements of the warrant,” which is then run across the records of searches conducted via Google Search and Maps.⁷⁵ At that point, Google “do[es] not know which, if any, users may have undertaken searches that would be responsive to the warrant in question,” and even if a user performed a relevant search during the specified time frame, the record might not exist anymore if it was deleted by the user.⁷⁶ Once Google executes the query, results are returned in a comma-separated values (CSV) file—a common format for storing large sets of data—listing all searches “containing the specified search term(s),” which may include the exact search term or additional words.⁷⁷

Next, Google *de-identifies* the raw query results by “truncat[ing] account-identifying information,” namely the full GAIA ID or the Browser Cookie ID.⁷⁸ A GAIA ID is an internal numeric identifier assigned to Google users who are signed in, whereas a Browser Cookie ID is assigned to searches performed without being signed into a Google account.⁷⁹ By truncating these IDs, Google removes enough characters to prevent the government from readily determining the account or device behind each query. This de-identified “production version” of the results still contains the date and time of the search, coarse location information (based on the approximate IP

70 Edano, *supra* note 7, at 981–82.

71 Guariglia, *supra* note 69.

72 See Winters, *supra* note 8, at 1370.

73 See Chan, *supra* note 7, at 284.

74 See Notice of Declaration of Legal Investigations Support Analyst ¶¶ 2–10, *People v. Seymour*, No. 21CR20001 (Colo. Dist. Ct. Aug. 16, 2022). Why are we only discussing what Google does? Although other search engines exist, Google dominates the market with nearly 92% of global usage (about 89% in the United States) and more than a billion monthly users. See Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Appellant and Reversal at 9, *Commonwealth v. Kurtz*, No. 98–100 MAP 2023 (Pa. Jan. 5, 2024). On average, it processes close to 100,000 queries every second—over 8.5 billion searches a day—and around 63% of those queries were conducted on mobile devices as of 2019. *Id.*

75 Notice of Declaration of Legal Investigations Support Analyst, *supra* note 74, ¶ 4.

76 *Id.* ¶ 5.

77 *Id.* ¶ 6.

78 *Id.* ¶ 7.

79 *Id.*

address), the search query the user entered, the result Google generated, the domain (such as google.com), and the portion of the URL that corresponds to the user's search request.⁸⁰ It also includes a truncated identifier—either a shortened GAIA ID or a shortened Browser Cookie ID—along with a “user agent string,” which typically indicates information like the browser type and operating system.⁸¹ With this limited yet meaningful technical information, law enforcement can determine whether a query is relevant without learning the user's identity.

Once the data is de-identified, Google provides these truncated results to law enforcement, who can then exclude irrelevant queries—such as those from different regions or those which fail to meet other key criteria.⁸² If the initial search warrant permits, the government can then require Google to disclose identifying information—such as IP addresses, full GAIA IDs, and basic subscriber information for users deemed relevant, and this mechanism applies both to truncated GAIA IDs and truncated Browser Cookie IDs.⁸³ However, if the warrant does not initially authorize obtaining such personal identifiers, Google will not turn over that data unless the government secures an additional warrant.⁸⁴ In sum, Google's process operates in two tiers: First, it provides de-identified results for law enforcement to identify relevant users; second, it discloses identifying information only with proper legal authority.

B. Recent Cases Involving Keyword Search Warrants

There is little that is publicly known about keyword search warrants.⁸⁵ In 2020, Richard Salgado, Google's Director of Law Enforcement and Information Security stated that keyword search warrants represent less than 1% of total warrants received by Google.⁸⁶ However, Google receives 60,000 to 70,000 search warrants a year,⁸⁷ and law enforcement's use of another type of reverse search warrant—the geofence warrant—increased over

80 *Id.*

81 *Id.*

82 *Id.* ¶ 8.

83 *Id.* ¶ 9.

84 *Id.*

85 Chan, *supra* note 7, at 284.

86 Jon Fingas, *Google Is Sharing User Data Tied to Search Keywords with Law Enforcement*, ENGADGET (Oct. 8, 2020, at 16:50 ET), <https://www.engadget.com/google-gives-search-keyword-user-data-to-police-144249434.html> [<https://perma.cc/TJY8-P3F5>].

87 Amanda Pampuro, *Colorado District Attorney Cannot Serve Google with Overbroad Reverse Search Warrant*, COURTHOUSE NEWS SERV. (Dec. 9, 2024), <https://www.courthousenews.com/colorado-district-attorney-cannot-serve-google-with-overbroad-reverse-research-warrant/> [<https://perma.cc/AH2V-6QST>].

1,000% in certain states between 2018 and 2020.⁸⁸ Thus, one can infer that law enforcement's use of keyword search warrants has also increased in recent years. Because little is publicly known about this type of warrant, there is very little case law or legal scholarship examining it. However, there were two recent state cases—one in the Colorado Supreme Court and one in the Pennsylvania Superior Court—that examined the constitutionality of this type of warrant.

1. *People v. Seymour*

The Colorado case, *People v. Seymour*, involved a warrant from the Denver police which requested that Google provide the IP addresses for any Google accounts used to conduct searches for a particular address (that was burned down in an arson attack) in the fifteen days preceding the fire.⁸⁹ Google disclosed five IP addresses to the Denver police that fit the warrant's criteria, and, using this information, law enforcement charged Gavin Seymour and two others with multiple counts of first-degree murder.⁹⁰ Seymour moved to suppress evidence obtained by the warrant, arguing that it lacked probable cause and particularity.⁹¹

In considering the motion to suppress, the Colorado Supreme Court first turned to the issue of whether the Denver police's request was even a search at all by applying the familiar two-pronged *Katz* test.⁹² Seymour had a subjective expectation of privacy in his Google search history, the court reasoned, because he did nothing to make his search data public and was correct in assuming that Google's method of storing user data would mean that his data would not be "broadcast to the world."⁹³ Turning to the second prong—whether an individual's expectation of privacy is objectively reasonable—the court first noted the similarities between an individual's Google search history and the CSLI location data from *Carpenter*.⁹⁴ Both CSLI and an individual's internet searches could reveal one's religious associations, private medical conditions, and other intimate details about their life.⁹⁵ In fact, an individual's search history reveals "as much, if not in many instances more, about one's private life than other records in which we've previously held individuals have a reasonable expectation of privacy."⁹⁶ Last, the court stated

88 Chad Marlow & Jennifer Stisa Granick, *Celebrating an Important Victory in the Ongoing Fight Against Reverse Warrants*, ACLU (Jan. 29, 2024), <https://www.aclu.org/news/privacy-technology/fight-against-reverse-warrants-victory> [<https://perma.cc/LP5C-5FSV>].

89 *People v. Seymour*, 536 P.3d 1260, 1267 (Colo. 2023).

90 *Id.*

91 *Id.*

92 *Id.* at 1270.

93 *Id.* at 1270, 1270–71 (quoting *People v. Gutierrez*, 222 P.3d 925, 932 (Colo. 2009)).

94 *Id.* at 1271.

95 *Id.*

96 *Id.* (citing *People v. Sporleder*, 666 P.2d 135, 143–44 (Colo. 1983)).

that the presence of digital privacy laws such as the Stored Communications Act demonstrates that society finds an expectation of privacy in digital data to be objectively reasonable.⁹⁷

However, the court was aware of Google's two-step process for responding to keyword search warrants.⁹⁸ It questioned whether the privacy interest in an individual's search history encompasses those histories when viewed "simply in connection with an anonymized IP address."⁹⁹ The court, while acknowledging that *Carpenter* has "cast[] some doubt on the [third-party] doctrine's overall reach," stated that most federal courts have generally held that an individual has no reasonable expectation of privacy in data that is provided to, and collected by, a third party.¹⁰⁰ Nevertheless, this is where the court's analysis "part[ed] ways with the Fourth Amendment," and it explained that Article II, Section 7 of the Colorado Constitution provides greater privacy protections than the Fourth Amendment.¹⁰¹ The court held that Seymour had a reasonable expectation of privacy in his Google search history even when viewed in connection with an IP address because the IP address "provides such a critical link in the chain of user identification."¹⁰²

Having concluded that law enforcement's request for Seymour's search data constituted a search under the Colorado Constitution, the court next turned to whether the warrant satisfied the requirements of particularity and probable cause. Emphasizing that the "ultimate touchstone" of the legality of a warrant is reasonableness, the court first held that the scope of the place to be searched—the first part of the particularity analysis—was reasonable when considering the search parameters provided in the warrant.¹⁰³ While the database that Google searched through for the relevant search terms was extremely large, "the narrow search terms, the timeframe constraints, and the fact that the initial search was anonymized" meant that there was no "rummaging" of the sort that the Founders feared.¹⁰⁴ As such, the place to be searched was not too broad. The court also stated that the warrant was adequately particularized with respect to the "things to be seized."¹⁰⁵ The warrant was clear that "only records containing one of the nine specified keywords were to be seized," and the executing officer had "virtually no discretion to determine which records" from Google's database were responsive.¹⁰⁶

97 *Id.*

98 *Id.* at 1271–72.

99 *Id.* at 1272, 1271–72.

100 *Id.* at 1272.

101 *Id.* (citing *People v. McKnight*, 446 P.3d 397, 406 (Colo. 2019))

102 *Id.*

103 *Id.* at 1275 (quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006)).

104 *Id.* at 1276 (citing *United States v. Place*, 462 U.S. 696, 705–07 (1983)).

105 *Id.* at 1277.

106 *Id.* at 1276.

The court, however, expressed some skepticism that the warrant satisfied probable cause. An invasion of someone's Fourth Amendment interests is only justified when there is *individualized* probable cause—satisfied only when there are specific and articulable facts directed to the person whose interests are being impinged.¹⁰⁷ In a previous case, the court had held that a warrant to search the financial records of nearly 5,000 individuals to check for those where the social security and individual tax ID numbers mismatched—a common indicator of undocumented status—lacked individualized probable cause in connection to the defendant whose file was one of the mismatches.¹⁰⁸ However, the court also recognized that Seymour's case was very different.¹⁰⁹ A computer searched through the database—rather than a human—looking only for an address.¹¹⁰ “The search was not concerned with who may have inquired; it did not seek the identity of any person; and it did not target any individual's documents.”¹¹¹ The court ultimately declined to decide the question of probable cause because it determined that the exclusionary rule's good-faith exception applied.¹¹² And because the good-faith exception applied, the court declined to suppress the evidence from the search.¹¹³

2. *Commonwealth v. Kurtz*

In the Pennsylvania case, *Commonwealth v. Kurtz*, law enforcement pursuing a rape investigation used a keyword search warrant to compel Google to provide them with the IP addresses of any Google searches of the victim's address in the week preceding the crime.¹¹⁴ Google returned a single IP address that was responsive to the requirements of the warrant.¹¹⁵ Law enforcement eventually connected this IP address to John Edward Kurtz, who was subsequently surveilled and arrested in connection with the

107 *Id.* at 1277.

108 *Id.* at 1277–78.

109 *Id.* at 1278.

110 *Id.*

111 *Id.*

112 John Villasenor, *Keyword Search Warrants and the Fourth Amendment*, BROOKINGS INST. (Feb. 22, 2024), <https://www.brookings.edu/articles/keyword-search-warrants-and-the-fourth-amendment/> [https://perma.cc/8ZE8-H4XR] (“Often, the ‘exclusionary rule’ blocks federal and state prosecutors from using evidence collected in a manner that violates the Fourth Amendment. But there is an exception: If a court finds that law enforcement acted in ‘good faith,’ the evidence can be presented at trial despite the constitutional violation. Invoking this good faith exception, the Colorado Supreme Court declined to suppress the evidence obtained using the keyword search warrant, concluding that ‘law enforcement obtained and executed the warrant in good faith.’” (quoting *Seymour*, 536 P.3d at 1268)).

113 *Id.*

114 *Commonwealth v. Kurtz*, 294 A.3d 509, 516–17 (Pa. Super. Ct. 2023).

115 *Id.* at 517.

crime.¹¹⁶ Kurtz sought to suppress the evidence of the Google searches conducted from his IP address.¹¹⁷

The court first held that Kurtz did not have a reasonable expectation of privacy in his Google searches of the victim's address in connection with his IP address.¹¹⁸ Because Kurtz typed his search query into the search engine, and pressed "Enter," he had "affirmatively turned over the contents of his search to Google . . . and voluntarily relinquished his privacy interest in the search."¹¹⁹ Further, Google's Privacy Policy explicitly states that it collects and shares users' search queries.¹²⁰ And Kurtz did not have a reasonable privacy interest in his IP address "because the IP address served as the manner in which Google's servers communicated with his computer."¹²¹ The court distinguished Kurtz's case from the collection of CSLI in *Carpenter* because Kurtz affirmatively chose to type in the victim's address and submit the search request in light of Google's policy of collecting and sharing user search queries.¹²² Moreover, unlike the "detailed chronicle" of an individual's movements that CSLI provides,¹²³ the warrant in question was limited in nature and did not "shed light on Appellant's political views, health information, or other sensitive matters."¹²⁴

The court then went on to conclude that even if there was a privacy interest in Kurtz's Google searches—and the Fourth Amendment's protections attached—the warrant still satisfied probable cause.¹²⁵ That was because it set forth grounds to demonstrate that there was a fair probability that the information from Google would uncover evidence related to the identity of the person who committed the crime.¹²⁶ There were many factors—the location of the attack, the timing of the attack, the motivation for the attack and the ubiquity of Google search—that reasonably led investigating officers to conclude that the crime was committed with significant planning and likely involved the use of Google's search engine.¹²⁷ However, the Court declined to address whether the warrant satisfied particularity.

116 *Id.*

117 *Id.* at 518.

118 *Id.* at 522.

119 *Id.* at 522 (first citing *Commonwealth v. Sodomsky*, 939 A.2d 363, 369 (Pa. Super. Ct. 2007); and then citing *Commonwealth v. Proetto*, 771 A.2d 823, 830–31 (Pa. Super. Ct. 2001)).

120 *Id.*

121 *Id.* (first citing *United States v. Christie*, 624 F.3d 558, 573–74 (3d. Cir. 2010); and then citing *Commonwealth v. Duncan*, 817 A.2d 455, 462–63 (Pa. 2003)).

122 *Id.*

123 *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018).

124 *Kurtz*, 294 A.3d at 522.

125 *See id.* at 524.

126 *See id.*

127 *Id.*

III. FOURTH AMENDMENT ANALYSIS OF KEYWORD SEARCH WARRANTS

A. *An Individual's Keyword Search Data Is Constitutionally Protected*

Law enforcement acquisition of an individual's keyword search data—even when the data is only provided in connection with a de-identified IP address—is a Fourth Amendment search. Although the *Carpenter* holding was narrow in that it only applied to historical CSLI, the *Carpenter* characteristics can be applied to other novel categories of information sought by law enforcement.¹²⁸ And these characteristics instruct us that this particular category of information—keyword search data—is constitutionally protected.

An individual's internet search queries are “deeply revealing”¹²⁹—even when linked only to an IP address. More so than historical CSLI, which merely pinpoints a person's location over an extended period, search queries lay bare a user's precise thoughts—captured in their own words—at a specific moment (and sometimes from a distinct location).¹³⁰ These searches can expose an individual's “familial, political, professional, religious, and sexual associations,”¹³¹ as well as how these associations evolve over time. Notably, in 2024, the top related topics for the query “Am I” were “menstruation” and “fatigue,” both of which implicate private health concerns.¹³² Professor Paul Ohm, in a hearing before the House Subcommittee on Communications and Technology, stated: “No power in the technological history of our nation has been able until now to watch us read individual articles, calculate how long we linger on a given page, and reconstruct the entire

128 In *Carpenter v. United States*, the Court emphasized three features of CSLI relevant to Fourth Amendment analysis: (1) its “deeply revealing nature”; (2) its “depth, breadth, and comprehensive reach”; and (3) the “inescapable and automatic nature of its collection.” See *supra* note 51 and accompanying text.

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

130 A recent survey of more than 3,000 Americans illustrates the depth of privacy concerns tied to internet search histories. Dani Henion, *How Far Would You Go to Keep Your Search History Private?*, SIMPLETEXTING: BEYOND TEXTING (May 31, 2022), <https://simpletexting.com/blog/search-history-privacy-survey/> [<https://perma.cc/NL9R-QDV5>]. According to the survey, 69% of respondents indicated that they would refuse to share their search history with their parents if asked, 55% would not share it with friends, and 28% would withhold it from a significant other. *Id.* Nearly three in ten respondents stated they would rather forgo their smartphones for an entire year than make their search histories public, and the average participant demanded over \$5.5 million in exchange for disclosing that information. *Id.*

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

132 GOOGLE TRENDS, “Am I” (Jan. 1, 2025) (on file with the Notre Dame Law Review) (filtered by “United States”, “2024”, “All categories”, “Web Search”, “Related topics”, “Top”).

intellectual history of what we read and watch on a minute-by-minute, individual-by-individual basis.”¹³³

Some courts, however, have cast doubt on whether IP address data is as revealing as historical CSLI. In *United States v. Kidd*, for example, the court concluded that a defendant lacked a protectable privacy interest in IP address data “because there is an insufficient record to support a conclusion that such information reflected the whole of [the defendant’s] locations and movements.”¹³⁴ Likewise, in *Heeger v. Facebook, Inc.* the court explicitly stated that “[t]here is no legally protected privacy interest in IP addresses alone.”¹³⁵ These opinions fail to acknowledge that, although an IP address by itself may not disclose as much as CSLI, the additional data commonly provided by search engine companies alongside that IP address—such as location, time, and the content of a search query¹³⁶—can arguably reveal more than historical CSLI. Moreover, as the court in *Seymour* observed, even an unidentified IP address, unconnected to personal account information, is not truly anonymous.¹³⁷ It still functions as a vital link in the chain of identifying a user because an Internet Service Provider (ISP) logs the IP address’s location information and any recognized services operating under that address.¹³⁸ Thus, an individual’s search query history—even when linked to a de-identified IP address—is “deeply revealing.”

An individual’s search query history data also possesses “depth, breadth and comprehensive reach,”¹³⁹ capturing a substantial degree of “detail and precision.”¹⁴⁰ Even when a user employs a de-identified IP address, Google and other search engines continue to collect device IDs, geolocation, time stamps, exact query terms, and ISP information¹⁴¹—data that may be

133 *FCC Overreach: Examining the Proposed Privacy Rules: Hearing Before the H. Subcomm. on Comm’n’s & Tech. of the H. Comm. on Energy & Com.*, 114th Cong. 29 (2016) (statement of Paul Ohm, Professor, Georgetown Univ. L. Ctr.).

134 *United States v. Kidd*, 394 F. Supp. 3d 357, 368 (S.D.N.Y. 2019).

135 *Heeger v. Facebook, Inc.*, 509 F. Supp. 3d 1182, 1190 (N.D. Cal. 2020).

136 *See supra* note 80 and accompanying text.

137 *See supra* note 102 and accompanying text.

138 Lukas Motiejunas, *How to Hide My IP Address in 2025: 5 Easy Ways*, OXYLABS (Jan. 1, 2025), <https://oxylabs.io/blog/how-to-hide-ip-address> [<https://perma.cc/A2EB-U38M>].

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

140 *See Winters, supra* note 8, at 1392 (“Depth refers to the detail and precision of the information stored.”).

141 *See* Daniel Law, *Does Google Track My Searches If I’m Not Signed In?*, RED SEARCH (July 5, 2023), <https://www.redsearch.com.au/resources/google-track-searches-not-signed-in/> [<https://perma.cc/XQ3J-6B68>]; *How Microsoft Stores and Maintains Your Search History*, MICROSOFT, <https://support.microsoft.com/en-us/windows/how-microsoft-stores-and-maintains-your-search-history-8742470a-9fb5-c05b-a2ad-5521cace2641> [<https://perma.cc/BTK4-SCXJ>] (last visited Mar. 23, 2025) (“When you search using Bing, Microsoft collects the search terms you provide, along with other information, such as your IP address and location, the unique identifiers contained in our cookies, the time and date of your search, and your browser configuration.”).

retained for several months.¹⁴² Given that almost every adult in the United States has used a search engine within the past four weeks,¹⁴³ and the average user conducts multiple searches daily,¹⁴⁴ these practices result in the accumulation of a “detailed log” of the vast majority of Americans’ thoughts, interests and inquiries over time.¹⁴⁵ Thus, in addition to its “depth,” search query data also has immense “breadth” and “comprehensiveness.”¹⁴⁶ And while search query data may not necessarily match the granularity of historical CSLI, that fact alone does not diminish its capacity to meet the threshold of depth, breadth, and comprehensiveness required to trigger Fourth Amendment protections.

The final *Carpenter* factor—whether the collection of information is “inescapable and automatic”—poses the greatest challenge to concluding that the collection of one’s search query history triggers Fourth Amendment scrutiny. IP address data is automatically generated whenever an individual uses the internet, and every person who employs a search engine necessarily generates search query data.¹⁴⁷ Admittedly, users can limit some of this data collection—for instance, by employing a virtual private network (VPN) to mask their local IP address, search queries, and browsing history.¹⁴⁸ Privacy-focused search engines such as DuckDuckGo and Startpage also promise not to track users’ searches or browsing activities.¹⁴⁹

142 *Save & Manage Search Activity*, GOOGLE WORKSPACE ADMIN HELP, <https://support.google.com/a/answer/11194328> [https://perma.cc/HQ4S-9MAR] (last visited Mar. 23, 2025) (“By default, Google deletes [search history] data after 18 months. However, . . . users can change the deletion period to 3, 18, or 36 months, or to never delete data.”).

143 Umair Bashir, *Share of U.S. Internet Users Who Used a Search Engine in the Past 4 Weeks in 2022, by Age*, STATISTA (July 9, 2025), <https://www.statista.com/statistics/479302/internet-users-who-used-a-search-engine-on-computer-within-the-last-month-usa/> [https://perma.cc/ZJM7-A7J5].

144 Meg Prater, *31 Google Search Statistics to Bookmark ASAP*, HUBSPOT (Oct. 22, 2024), <https://blog.hubspot.com/marketing/google-search-statistics> [https://perma.cc/E3B2-8QX6] (“The number of yearly Google queries is in the trillions, and the average person conducts 6.8 searches per day.”).

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

146 See Winters, *supra* note 8, at 1392, 1395 (“Breadth refers to how frequently the data is collected and how long the data has been recorded Comprehensive reach refers to the number of people tracked in the database.” *Id.* at 1392.).

147 *IP Address Explained: What Is an IP Address?*, INTUIT MAILCHIMP, <https://mailchimp.com/resources/ip-address-explained/> [https://perma.cc/3ST9-4VSW] (last visited Mar. 23, 2025).

148 *What Is a VPN and Can It Hide My IP Address?*, MCAFEE, <https://www.mcafee.com/learn/what-is-a-vpn-and-can-it-hide-my-ip-address/> [https://perma.cc/2ZU7-H7SF] (last visited Mar. 23, 2025).

149 *How Does DuckDuckGo Protect My Privacy?*, DUCKDUCKGO, <https://duckduckgo.com/duckduckgo-help-pages/company/how-does-duckduckgo-protect-privacy/> [https://perma.cc/585W-8PVY] (last visited Mar. 23, 2025); *How It Works: The Startpage Difference*, STARTPAGE, <https://www.startpage.com/en/how-startpage-works/> [https://perma.cc/3VXE-9DRY] (last visited Mar. 23, 2025).

Yet these possibilities do not negate broader practical realities. More than half of Americans do not use a VPN, and of those who do, nearly half rely on free VPNs that may compromise data security.¹⁵⁰ Some paid VPNs likewise retain user information, permitting law enforcement to monitor keyword searches.¹⁵¹ Moreover, while one could theoretically avoid search query data collection by using alternative search engines, Google and Bing together hold over 94% of the U.S. market.¹⁵² Privacy-oriented search engines often entail substantial performance trade-offs, making it difficult to participate fully in modern online life—even for those who value privacy.¹⁵³

Courts have also suggested that using the internet—and thus generating IP address data—is a voluntary act of conveying information to a third party, which would place it beyond Fourth Amendment protections.¹⁵⁴ This view, however, overlooks the ubiquity and practical necessity of both the internet and search engines in daily life. In *Carpenter*, the Supreme Court treated historical CSLI as *practically* inescapable because one would need to power down or disconnect a phone from the cell network to avoid data collection¹⁵⁵—an untenable solution in the modern world. Likewise, expecting an individual to forgo the internet or search engines entirely is similarly impractical for meaningful participation in contemporary society.¹⁵⁶ To require total inescapability would render this factor meaningless, since “[v]irtually every form of digital surveillance is escapable with sufficient effort.”¹⁵⁷ Consequently, the near-universality and necessity of internet usage render search

150 Brett Cruz, *2024 VPN Use in 2025: Trends, Statistics, and Consumer Sentiment*, SECURITY.ORG (July 21, 2025), <https://www.security.org/resources/vpn-consumer-report-annual/> [<https://perma.cc/TT33-QMP6>].

151 See Aliza Vigderman & Gabe Turner, *Do VPNs Hide My Browsing History?*, SECURITY.ORG (Feb. 12, 2025), <https://www.security.org/vpn/browsing-history/> [<https://perma.cc/85HN-E672>]; Sam Singleton, *VPNs and the Law: How Often Does Law Enforcement Actually Request VPN Logs?*, PCWORLD (June 17, 2024, 6:00 PT), <https://www.pcmag.com/article/2367508/vpns-and-the-law-how-often-does-law-enforcement-actually-request-vpn-logs.html> [<https://perma.cc/QSA6-5QBW>].

152 See *Search Engine Market Share United States of America*, STATCOUNTER, <https://gs.statcounter.com/search-engine-market-share/all/united-states-of-america> [<https://perma.cc/J428-9KYE>] (last visited Mar. 23, 2025).

153 See Sam Hollingsworth, *DuckDuckGo vs. Google: An In-Depth Search Engine Comparison*, SEARCH ENGINE J. (May 21, 2021), <https://www.searchenginejournal.com/google-vs-duckduckgo/301997/> [<https://perma.cc/LJ6W-VC5V>].

154 See *United States v. Soybel*, 13 F.4th 584, 592–94 (7th Cir. 2021); *United States v. Hood*, 920 F.3d 87, 92 (1st Cir. 2019).

155 See *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018).

156 See *id.* at 2262 (2018) (Gorsuch, J., dissenting) (“Today we use the Internet to do most everything.”); *United States v. Gonyea*, Nos. 22-1722-cr, 22-1727-cr, 2023 WL 7478489, at *2 (2d Cir. Nov. 13, 2023) (“As early as 2001, we observed that ‘[c]omputers and Internet access have become virtually indispensable in the modern world of communications and information gathering.’” (alteration in original) (quoting *United States v. Peterson*, 248 F.3d 79, 83 (2d Cir. 2001))).

157 Matthew Tokson, *Inescapable Surveillance*, 106 CORN. L. REV. 409, 426 (2021).

query data collection—tied even to a mere IP address—practically inescapable and automatic.

Lower court decisions interpreting *Carpenter* also indicate that these characteristics function more as a flexible guide than a rigid test.¹⁵⁸ Among these characteristics, the revealing nature of the data has emerged as the most influential.¹⁵⁹ Courts have given less consideration to whether the data is truly inescapable or how many people it affects.¹⁶⁰ As the preceding discussion shows, search query data—particularly when combined with location and time details—can expose more intimate information than historical CSLI, revealing private thoughts, interests, and health concerns. Although it remains unsettled whether search query data matches the inescapable quality of the CSLI at issue in *Carpenter*, courts have not treated any shortfall in that regard as dispositive in determining whether such data is constitutionally protected.¹⁶¹ Because of its unparalleled capacity to illuminate users' personal lives, the collection of keyword search data—even when tied only to an IP address—qualifies as a Fourth Amendment search under the *Carpenter* framework.

B. Keyword Search Warrants Are Not Categorically Unconstitutional

Once Fourth Amendment protections attach to a law enforcement request for information, a warrant that satisfies probable cause and particularity is required.¹⁶² And a particular type of warrant can only be categorically unconstitutional if it will *never* be able to satisfy these twin requirements. Some scholars and public interest groups maintain that keyword search warrants fall into this category.¹⁶³ This Note takes the opposite view. Keyword searches are not categorically unconstitutional because it is possible for them to be drawn narrowly enough to satisfy both probable cause and particularity.

1. Probable Cause

To satisfy probable cause with their warrant, law enforcement need only demonstrate that there is a “fair probability” that evidence or suspects to a crime will be found in the information that the law enforcement agency requests.¹⁶⁴ Further, the facts alleged in the warrant should demonstrate that

158 See Tokson, *supra* note 53, at 1825 tbl. 4.

159 See *id.*

160 See *id.*

161 See *id.*

162 See *supra* note 54 and accompanying text.

163 See, e.g., Chan, *supra* note 7, at 299; Edano, *supra* note 7, at 1000–02; Press Release, Elec. Frontier Found., EFF Urges Pennsylvania Supreme Court to Find Keyword Search Warrant Unconstitutional, (Jan. 5, 2024), \ <https://www.eff.org/press/releases/eff-urges-pennsylvania-supreme-court-find-keyword-search-warrant-unconstitutional> [<https://perma.cc/TY74-C8VS>].

164 See *supra* note 56 and accompanying text.

the IP addresses sought will aid in a “particular apprehension” for “a particular offense.”¹⁶⁵ It is difficult to imagine that *every* keyword search warrant would fail to meet this threshold. Consider *Kurtz* as a prime example of a narrowly drawn warrant that satisfied probable cause. There, the Court upheld a keyword search warrant on the grounds that it presented specific and articulable facts—such as the remote location of the victim’s residence and the site where the victim was ultimately dropped—that demonstrated the crime had been carefully orchestrated.¹⁶⁶ Given Google’s ubiquity as a search engine, it was reasonable to conclude that this planning was likely conducted via Google’s search engine. This was more than enough to determine that there was a “fair probability” that one of the IP addresses requested—those that searched for the victim’s name or home address in the seven days preceding the attack—would be the perpetrator of the crime.¹⁶⁷ And there are many other hypothetical scenarios where there would likely be probable cause in the facts alleged in the keyword search warrant—for instance, where a suspect in an arson investigation made online inquiries about specialized accelerants days before the fire, or where an individual repeatedly queried personal information corresponding to a known identity-theft victim in the period leading up to the alleged theft. Thus, it is possible for probable cause to be satisfied in at least some keyword search warrants.

2. Particularity

The place to be searched must be particular for a warrant to be valid under the Fourth Amendment.¹⁶⁸ At first glance, it may seem that the place to be searched cannot be particular since it will entail querying a search engine company’s entire database for certain keywords. Indeed, the Fifth Circuit appeared to adopt this reasoning in a recent geofence-warrant decision, which likewise involved searching an enormous amount of data for relevant entries.¹⁶⁹ The Fifth Circuit stated that geofence warrants “allow law enforcement to rummage through troves of location data from hundreds of millions of Google users without any description of the particular suspect or suspects to be found.”¹⁷⁰ And even though Google, a private party, is the one initiating the query and returning the results to law enforcement, the Fifth Circuit, in a footnote, stated that “the Fourth Amendment protects against *both* searches

165 *Dalia v. United States*, 441 U.S. 238, 255 (1979) (quoting *Warden v. Hayden*, 387 U.S. 294, 307 (1967)).

166 *See supra* notes 125–27 and accompanying text.

167 *Commonwealth v. Kurtz*, 294 A.3d 509, 523 (Pa. Super. Ct. 2023) (quoting *Commonwealth v. Harlan*, 208 A.3d 497, 505 (Pa. Super. Ct. 2019)).

168 *See supra* note 59 and accompanying text.

169 *See United States v. Smith*, 110 F.4th 817, 837–38 (5th Cir. 2024).

170 *Id.*

and seizures ‘effected by a private party . . . if the private party acted as an instrument or agent of the Government.’”¹⁷¹

However, the Fifth Circuit’s holding is hard to square with *United States v. Carpenter*. The Court in *Carpenter* stated that the search occurred “when the Government accessed CSLI from the wireless carriers.”¹⁷² Although the cell provider filtered through its entire database to locate the requested CSLI, law enforcement ultimately received only the subset of records authorized by the warrant.¹⁷³ And it is only this subset that is relevant for the particularity analysis. *Carpenter* also held that a warrant, rather than a subpoena, was required to compel cell carriers to hand over CSLI.¹⁷⁴ As Professor Orin Kerr points out, “[m]ost searches for *Carpenter*-protected data will be through massive databases. If the governing law is that a warrant is sufficient (the Supreme Court rule) except when the database queried is massive (the Fifth Circuit’s rule), in practice that amounts to a rejection of the Supreme Court’s holding in *Carpenter*.”¹⁷⁵ Thus, in multiple respects, the Fifth Circuit’s stance—that a private party’s front-end search through its entire database necessarily undermines particularity—cannot be reconciled with *Carpenter*’s allowance for warrant-based retrieval from large data repositories.

The Supreme Court has also stated that “it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized” and “officials . . . must take care to assure that [searches] are conducted in a manner that minimizes unwarranted intrusions upon privacy.”¹⁷⁶ Here, when a search engine company runs a keyword query across its database, the process is automated—neither law enforcement nor the provider’s staff ever views records unrelated to the warrant’s terms.¹⁷⁷ Although the system necessarily scans countless benign entries, these unresponsive records remain unseen by human eyes. This automated approach thus avoids the kind of indiscriminate

171 *Id.* at 838 n.12 (omission in original) (quoting *Skinner v. Ry. Lab. Execs.’ Ass’n*, 489 U.S. 602, 614 (1989)). *But see* *United States v. Davis*, 109 F.4th 1320, 1331 (11th Cir. 2024) (“The Constitution is not concerned with a private party’s search of its own records.” (first citing *Walter v. United States*, 447 U.S. 649, 656 (1980); and then citing *United States v. Chatric*, 107 F.4th 319, 330 n.16 (2024), *aff’d en banc*, 136 F.4th 100 (4th Cir. 2025))).

172 *Carpenter v. United States*, 138 S. Ct. 2206, 2219 (2018) (emphasis added).

173 *See id.* at 2226 (Kennedy, J., dissenting).

174 *Id.* at 2221.

175 Orin Kerr, *The Fifth Circuit Shuts Down Geofence Warrants—and Maybe a Lot More*, LAWFARE (Aug. 14, 2024, 08:00), <https://www.lawfaremedia.org/article/the-fifth-circuit-shuts-down-geofence-warrants-and-maybe-a-lot-more> [<https://perma.cc/3LZQ-T5SR>].

176 *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976).

177 *See* *People v. Seymour*, 536 P.3d 1260, 1276 (Colo. 2023) (“No human, let alone any law enforcement official, saw information falling outside the warrant’s narrow search parameters.”); *see also* Orin S. Kerr, *Data Scanning and the Fourth Amendment*, 67 B.C. L. REV. 431, 452–53 (2026).

rummaging that alarmed the Founders and gave rise to the Fourth Amendment's protections.

Finally, as the court in *Seymour* pointed out, the “ultimate touchstone” of the legality of a warrant is reasonableness.¹⁷⁸ It seems perfectly reasonable to ask a search engine company, like Google, for very limited information related to a criminal investigation—information that can only be collected using a computer to filter through a larger database. If this were held to be unreasonable, then *any* information in a database large enough could not be searched, even with a warrant. Aside from the perverse incentives this creates, it would also have profound implications for national security programs and many other law enforcement surveillance programs and practices.¹⁷⁹

Instead, the particularity of the area to be searched should be analyzed in relation to the constraints placed upon the information requested. In *United States v. Karo*, the Court acknowledged that a warrant could still be sufficiently particular even if the “place” to be searched—in that case, any future location the suspect’s beeper-equipped vehicle might visit—was effectively open-ended.¹⁸⁰ Although such a scope appeared to encompass “everywhere,” a warrant with appropriate constraints on the intended use of the beeper would have satisfied particularity.¹⁸¹ Similarly, a keyword search warrant may entail combing through the provider’s entire corpus of user queries from a given period—potentially encompassing all searches made over several months.¹⁸² However, as in *Karo*, it is possible to constrain the request in the warrant to limit the search to very specific keywords, time periods, and locations so that the “place” to be searched is much smaller than the entirety of the database. It is then *possible* for a keyword search warrant to satisfy the particularity as to the “place” or area to be searched.

The second part of the particularity analysis is that the warrant must be particular as to the items or people to be seized.¹⁸³ In other words, how broad can the warrant be drawn? Again, it is hard to imagine that no warrant can be drawn narrowly enough to pass constitutional muster. Keyword search warrants *can* be very narrow and targeted. In *Seymour*, for example, Google only returned a spreadsheet of sixty-one searches made by eight accounts as a result of “the narrow search terms [and] timeframe constraints” in the warrant.¹⁸⁴ It is thus *possible* that some keyword search warrants can satisfy the particularity requirements as to the items or people to be seized.

Some scholars argue that keyword search warrants cannot satisfy this aspect of the particularity analysis because the suspect is unknown and

178 *Seymour*, 536 P.3d at 1275 (quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006)).

179 *See* Kerr, *supra* note 175.

180 *See* *United States v. Karo*, 468 U.S. 705, 718 (1984).

181 *Id.*

182 *See generally supra* note 142.

183 *See supra* notes 66–68 and accompanying text.

184 *People v. Seymour*, 536 P.3d 1260, 1276 (Colo. 2023).

cannot be described.¹⁸⁵ However, it is irrelevant whether the suspect is known. For example, the Court in *Zurcher v. Stanford Daily* approved a warrant to search a newspaper's headquarters for photos of a campus protest to identify suspects even though the warrant did not name or describe any of the suspects.¹⁸⁶ Indeed, the *whole purpose* of the keyword search warrant is to identify suspects. And there are plenty of other instances of courts upholding warrants seeking to identify suspects despite not knowing who they are.¹⁸⁷

CONCLUSION

Keyword search warrants lie at the intersection of investigative need and digital privacy. They are Fourth Amendment “searches,” so constitutional safeguards attach, but they are not per se invalid: Warrants cabined by precise terms, dates, and other limits can satisfy probable-cause and particularity requirements. Uncertainty persists over how broadly they may sweep and what privacy costs they impose. Because the Fourth Amendment sets only a floor, Congress and state legislatures can—and arguably should—raise the bar by requiring stricter procedures or tighter scopes. Such legislation would better balance effective policing with privacy as data-collection technologies rapidly evolve.

185 See, e.g., Edano, *supra* note 7, at 1001 (“[O]fficers cannot particularize keyword warrants because the context behind a search is not necessarily connected to a specific perpetrator.”); Chan, *supra* note 7, at 300 (“Keyword search warrants are unconstitutional because they do not describe a known individual.”).

186 See *Zurcher v. Stanford Daily*, 436 U.S. 547, 555 (1978); see also *In re Search of Info. that is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d 62, 83 n.19 (D.D.C. 2021) (“[T]he Fourth Amendment does not and has never required that law enforcement know a suspect’s identity for certain or even have a suspect in mind to obtain a search warrant.”).

187 See, e.g., *United States v. Easterday*, 712 F. Supp. 3d 46, 53 (D.D.C. 2024) (upholding a geofence warrant even though the warrant “did not draw a connection between . . . the [geofence] data [requested] and [the suspect] specifically”); *United States v. Morris*, No. 20-CR-100 2022 WL 1651408, at *11 (W.D.N.Y. Apr. 12, 2022) (denying a motion to suppress evidence obtained from a warrant for CSLI whose affidavit did not identify a suspect); see also Kerr, *supra* note 175 (“[I]t’s hard to imagine a contrary rule. I mean, *most* warrants for internet investigations are to identify a suspect.”).