Washington Law Review

Volume 97 | Number 4

12-1-2022

Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants

Chelsa Camille Edano
University of Washington School of Law

BEWARE WHAT YOU GOOGLE: FOURTH AMENDMENT CONSTITUTIONALITY OF KEYWORD WARRANTS

Chelsa Camille Edano*

Abstract: Many Americans have potentially had their privacy rights invaded through invisible, widespread police searches. In recent years, local and federal governments have compelled Google and other search engine companies to produce the personal information of users who have conducted a search query related to a crime. By using keyword warrants, the government can conduct a dragnet search for suspects, imposing suspicion on users and exposing their personal information. The keyword warrant is a symptom of the erosion of the Fourth Amendment protection against suspicionless searches. Not only is scholarship scarce on keyword warrants, but also instances of these warrants are rare because the court often seals the records. This Comment argues that keyword warrants are unconstitutional under the Fourth Amendment because these warrants do not meet the particularity requirement, which requires warrants to name the place or person to be searched. Here, keyword warrants cast a wide net on potentially thousands of individuals. In response, technology companies should be more involved in fighting to secure the personal information of their users, not only for their customers' benefit, but to protect the integrity of their product. Additionally, while courts should be striking down keyword warrants, this Comment advises legislatures to curb the government's use of essential technologies, like search engines, as a means of surveillance.

INTRODUCTION

In October 2020, the Denver Police Department hit a wall. The Department was investigating an arson at a home of eight individuals, killing five who were trapped inside.[1] Police executed at least twenty-three search warrants, four of which searched through thousands of people's locations via their mobile devices.[2] Yet still, police officers could not pinpoint their suspect.[3] Police then decided to follow in the footsteps

* J.D. Candidate, University of Washington School of Law, Class of 2023. Thank you to my editors, Emma VanderWeyst, Christopher Marelich, and Sabrina Suen; my advisor, Professor Mary D. Fan; and my family, especially my mama and Chrysia. Surviving the long caffeine-fueled nights would not be possible without Angela K. Chen, Anna Le, Kyler Teo, and Biscotti.

1. 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), 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=6a49d46b6608 [https://perma.cc/LX2Q-4GAR].

2. Motion to Suppress Evidence from a Keyword Warrant & Request for a Veracity Hearing at 3–4, People v. Seymour, No. 21CR20001 (D. Colo. June 30, 2022) [hereinafter Motion to Suppress].

3. *Id.*

of other departments around the nation;[4] they filed three warrants to uncover any Google searches that included the address of where the fire occurred.[5]

Privacy analysts labeled these warrants, which force search engines to provide personal information on anyone who may have inputted certain terms, "keyword warrants."[6] Despite not being found through twenty-three other searches, three new individuals were implicated through this keyword search.[7] One of these suspects is Gavin Seymour.[8] Mr. Seymour is now the first defendant to mount a constitutional challenge against keyword warrants by moving to suppress the evidence obtained through the warrant.[9] As of September 2022, the judge has yet to rule on Mr. Seymour's motion.[10]

Every second, internet users around the world conduct an estimated 63,000 searches on Google.[11] Unbeknownst to most of us, however, we are leaving internet footprints about our thoughts, our whims, and our curiosities for the government to surveil, without our consent or our knowledge. As search engines and the internet become more accessible[12] and ingrained into our daily lives, authorities gain more ways to intrude in spaces we believed were private. Due to the expanding utility of these widespread searches in police investigations, keyword warrants are an emerging tool that will become more widespread if left unchecked.

This Comment analyzes the federal constitutionality of keyword warrants and the role of reverse search warrants in dragnet policing. Dragnets within the policing context are defined as the government investigation of a group of people, who are mostly presumably innocent,

---

4. 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) [hereinafter Brewster, *Exclusive: Government Secretly Orders Google*], https://www.forbes.com/sites/thomasbrewster/2021/10/04/google-keyword-warrants-give-us-government-data-on-search-users/?sh=3c7f9d5d7c97 [https://perma.cc/2GB4-8ADX].

5. Motion to Suppress, *supra* note 2, at 3–4.

6. Brewster, *Exclusive: Government Secretly Orders Google*, *supra* note 4.

7. Motion to Suppress, *supra* note 2, at 3–4.

8. *Id.*

9. Brewster, *supra* note 1.

10. Matt Jablow, *Crucial Hearing Held in Deadly Colorado Arson Case*, 9NEWS (Aug. 19, 2022), https://www.9news.com/article/news/crime/true-crime/diol-family/diol-family-arson-case-court-hearing/73-f51129a8-ebef-4c23-a5d4-619a421853a0 [https://perma.cc/UBA4-LUCD].

11. Danny Sullivan, *Google Now Handles At Least 2 Trillion Searches per Year*, SEARCH ENGINE LAND (May 24, 2016), https://searchengineland.com/google-now-handles-2-999-trillion-searches-per-year-250247 [https://perma.cc/MT54-L79T].

12. *Internet/Broadband Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021) [hereinafter *Internet/Broadband Fact Sheet*], https://www.pewresearch.org/internet/fact-sheet/internet-broadband/ [https://perma.cc/PC4Z-MWP6].

to fish out a few bad actors.[13] Part I begins with a general discussion of the machinations of search engines and how the data retrieved by these engines serve as the fuel to obtain keyword warrants. Keyword warrants compel search engines to hand over the personal data of users who have searched specific terms, within a certain timeframe, sometimes within a certain area. Section II.A delves into the history of the Fourth Amendment and its ties to privacy and security in the digital age. The historical abuse of general warrants, warrants that allow law enforcement to search unspecified places or seize unspecified people,[14] shapes the restrictions on the government imposed by the Fourth Amendment. The public does not know the full scope of keyword warrants, as they are relatively new and some are filed under seal,[15] resulting in little or no litigation or scholarship on the subject. Therefore, this Comment draws analogies to cell tower dumps and geofence warrants, which have been hotly litigated, within section II.B. Despite some courts upholding these types of "reverse search warrants," section III.A argues that keyword warrants are categorically unconstitutional under the Fourth Amendment and jeopardize American privacy rights because keyword warrants are inherently more invasive than tower dump and geofence warrants, and do not meet the standards of particularization required of a warrant. Section III.B seeks ways that corporations can mitigate the harm done by suspicionless searches for their users' benefit and their own, and section III.C calls on the legislature to step in to protect Fourth Amendment rights.

I. KEYWORD WARRANTS AND ACCESSING MASSIVE AMOUNTS OF PERSONAL DATA

Law enforcement officers issue search warrants, orders to search for evidence in a specific place, because they already have a suspect in mind.[16] However, keyword warrants compel search engine companies to provide information on users who have searched specific words, so that they may then find suspects.[17] Google, the most popular search engine,[18] retains data on users' identities and what users search, making it the ideal

13. Christopher Slobogin, *Government Dragnets*, 73 L. & CONTEMP. PROBS. 107, 108 (2010).

14. Hon. M. Blane Michael, *Reading the Fourth Amendment: Guidance from the Mischief that Gave It Birth*, 85 N.Y.U. L. REV. 905, 909 (2010).

15. Brewster, *Exclusive: Government Secretly Orders Google*, *supra* note 4.

16. *See infra* Part II.

17. Brewster, *Exclusive: Government Secretly Orders Google*, *supra* note 4.

18. *Internet Health Report 2018: More than 90% of the World Uses Google Search*, MOZILLA (Apr. 2018) [hereinafter *Internet Health Report 2018*], https://internethealthreport.org/2018/90-of-the-world-uses-google-search/ [https://perma.cc/LP52-SD2S]. This Comment chooses to focus specifically on Google due to the prolific nature and near dominance of Google as a search engine.

target of these warrants. As a result, law enforcement offices around the nation have used keyword warrants to conduct extensive digital searches for suspects.

A. Search Engines Are a Treasure Trove of Private Information

Keyword warrants are an increasingly popular tool for law enforcement because police can search through a space used by a vast number of individuals. Ninety-three percent of American adults use the internet.[19] To access the internet, users launch a web browser, which connects them to various websites.[20] If the user does not know which website to go to or seeks information about a topic, users can go to a search engine, which "locate[s] key words in other sites."[21] When internet users attempt to locate a website or input a search query, they almost always go to Google, which retains around 90% of the global market share for search engines.[22] As soon as a user conducts a search on Google, Google's automated systems sort through billions of webpages in Google's search index and screen for the most relevant content—all in the span of a fraction of a second.[23] Google also logs a user's queries into a search history list.[24] While this list is convenient, allowing users to look up what they have searched in the past, it also informs which advertisements, applications, and other content are recommended to them.[25] Many internet users, however, do not know how to limit the information a website collects on them.[26]

For most users, Google is their go-to option. Because Google has dominated the search engine industry for so long, the company has amassed an index of over 500 million webpages, dwarfing its

---

19. *Internet/Broadband Fact Sheet*, *supra* note 12.

20. *What Is a Web Browser?*, MOZILLA, https://www.mozilla.org/en-US/firefox/browsers/what-is-a-browser/ [https://perma.cc/KHH7-R2LD].

21. *Search Engine*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/search%20engine [https://perma.cc/W585-A3HX].

22. *Internet Health Report 2018*, *supra* note 18.

23. *How Google Search Works*, GOOGLE SEARCH, https://www.google.com/search/howsearchworks/how-search-works/ [https://perma.cc/8EGS-LBYH].

24. *Id.*

25. *Google Privacy Policy*, GOOGLE, https://www.gstatic.com/policies/privacy/pdf/20210701/7yn50xee/google_privacy_policy_en_us.pdf [https://perma.cc/7P39-ZGCW].

26. Kristen Purcell, Joanna Brenner & Lee Rainie, *Search Engine Use 2012: Main Findings*, PEW RSCH. CTR. (Mar. 9, 2012), https://www.pewresearch.org/internet/2012/03/09/main-findings-11/ [https://perma.cc/KVA3-3MM4].

competitors.[27] There are few other alternatives. Bing, an alternative search engine created and operated by Microsoft, is the default search engine on Windows personal computers, using the web browser Microsoft Edge.[28] Bing, second to Google, retains 5.8% of the search engine market share worldwide as of 2017.[29] Additionally, the Department of Justice has filed suit against Google, accusing it of engaging in monopolistic practices that guide users to its search engine.[30] With little (and sometimes no) choice, users are funneled into using Google search. This rings true especially for communities of color and communities with older or poorer populations, which are disparately impacted because these marginalized communities are less likely to have the generational resources to invest in the level of digital literacy[31] that is comparable to the rest of the population.[32] In fact, users with less technical familiarity often do not engage in or engage in less effective practices that control the privacy of their personal information online.[33] Even if users do have experience with online services, that experience may not be helpful when the privacy policies provided by major technology companies and media platforms are vague and incomprehensible.[34]

Google retains incredibly detailed personal data.[35] Google collects

---

27. Daisuke Wakabayashi, *Google Dominates Thanks to an Unrivaled View of the Web*, N.Y. TIMES (Dec. 14, 2020), https://www.nytimes.com/2020/12/14/technology/how-google-dominates.html (last visited Nov. 3, 2022).

28. *Internet Health Report 2018*, *supra* note 18.

29. *Id.*

30. These monopolistic practices include pre-installing Google search on devices and requiring certain web browsers to default to Google search. Complaint at 3–7, United States v. Google LLC, No. 1:20-cv-03010 (D.C. Cir. Oct. 10, 2020).

31. Digital illiteracy is classified by the Program for the International Assessment of Adult Competencies as adults "who reported no computer use, who were unwilling to take the assessment on the computer, or who failed the basic computer test." Saida Mamedova & Emily Pawloski, *Stats in Brief: A Description of U.S. Adults Who Are Not Digitally Literate*, 161 U.S. DEP'T OF EDUC.: NAT'L CTR. FOR EDUC. STAT. 2 (2018), https://nces.ed.gov/pubs2018/2018161.pdf [https://perma.cc/NN3U-ZUXE].

32. *Id.*

33. Yong Jin Park, *Digital Literacy and Privacy Behavior Online*, 40 COMMC'N RSCH. 215, 230 (2011).

34. Kevin Litman-Navarro, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, N.Y. TIMES (Aug. 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html (last visited Nov. 3, 2022). Google's privacy policy was a thirty-minute read in 2018, when the European Union's General Data Protection Regulation went into effect that required policies to be in clear and plain language. In 2019, Google's policy became much shorter when Google got rid of a glossary of technical terms. *Id.*

35. DOUGLAS C. SCHMIDT, DIGIT. CONTENT NEXT, GOOGLE DATA COLLECTION (2018), https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf [https://perma.cc/NC5A-MASJ].

personal identifiers (name, phone number, and address), demographic information, commercial information, biometric information (if provided), internet and network information (search terms, content and advertisement views, interaction with applications, browsers, devices, IP addresses,[36] and activity on third-party sites that use Google services), geolocation data, voice and audio information (if provided), professional or educational information (if using an account maintained through an organization), photos and videos, and emails and documents.[37] Google generally protects private information by only allowing the user to see this data and shielding user data from "unauthorized access, alteration, disclosure, or destruction of information" Google keeps.[38] As of 2020, Google began automatically deleting users' location history and web and application activity after eighteen months for newly created accounts.[39] However, certain actors, such as national or international governments, can demand user information, and law enforcement has increasingly used third party subpoenas and warrants to seek personal user information.[40]

Google claims to push back against warrants and government requests to disclose user data "when a request appears to be overly broad or doesn't follow the correct process."[41] Google states that "if a request asks for too much information, [Google] tr[ies] to narrow it, and in some cases [Google] object[s] to producing any information at all."[42] Indeed, in 2006, Google was the only search engine to resist a subpoena by the federal government to hand over the search histories of all of its users in order to

---

36. An IP address is an internet protocol address, a unique series of numbers that are connected to a computer, allowing it to be located by other machines. Eduardo R. Mendoza, *Network Investigation Techniques: Government Hacking and the Need for Adjustment in the Third-Party Doctrine*, 49 ST. MARY'S L.J. 237, 243–44 (2017).

37. *Google Privacy Policy*, *supra* note 25, at 4.

38. *Id.* at 13.

39. Alfred Ng & Richard Nieva, *Google Makes Auto-Deleting Data the Default for New Accounts*, CNET (May 27, 2020), https://www.cnet.com/news/privacy/google-makes-auto-deleting-data-the-default-for-new-accounts/ [https://perma.cc/D8UL-CD4N].

40. Jayni Foley, *Are Google Searches Private? An Originalist Interpretation of the Fourth Amendment in Online Communication Cases*, 22 BERKELEY TECH. L.J. 447, 451 (2007).

41. *Google Privacy Policy*, *supra* note 25, at 26; Sidney Fussell, *An Explosion in Geofence Warrants Threatens Privacy Across the US*, WIRED (Aug. 27, 2021) [hereinafter Fussell, *An Explosion in Geofence Warrants*], https://www.wired.com/story/geofence-warrants-google/ [https://perma.cc/WTV4-XMS7] ("'We vigorously protect the privacy of our users while supporting the important work of law enforcement,' Google said in a statement to WIRED. 'We developed a process specifically for these requests that is designed to honor our legal obligations while narrowing the scope of data disclosed.'").

42. *Global Requests for User Information*, GOOGLE TRANSPARENCY REP., https://transparencyreport.google.com/user-data/overview [https://perma.cc/3CVY-P9KP].

assist in its investigation into online pornography.[43]

It is difficult for users to fight back against these warrants because users do not usually know if Google is accessing their information or giving it to the government. Google and other technology companies do not usually notify users if or when the government reviews their data, as most warrants issued contain a non-disclosure clause.[44] In 2020 alone, Google received 38,132 search warrant requests in the United States, and Google disclosed information for about 82% of those requests.[45]

Similar to Google, Microsoft collects an abundance of personal information through Bing search, and because Windows owns most of the worldwide computer market share, most computer-users have access to Bing.[46] There are no specific numbers for Bing search, but in 2020, Microsoft received 48,891 law enforcement requests, and disclosed non-content data for more than 50% of the requests and content data for around 5% of requests.[47] After Bing, Yahoo Search holds 3% of the search engine market share on desktop computers.[48] Yahoo received 26,260 total government data requests in 2020.[49] Like both Google and Microsoft, Yahoo claims to "narrowly interpret the request and disclose only as much data as is necessary to comply with the request."[50]

In response, states have taken the initiative to implement comprehensive consumer data privacy laws, providing individuals the "right to access and delete personal information" and requirements for online services to create a transparent privacy policy.[51] California

---

43. Katie Haffner & Matt Richtel, *Google Resists U.S. Subpoena of Search Data*, N.Y. TIMES (Jan. 20, 2006), https://www.nytimes.com/2006/01/20/technology/google-resists-us-subpoena-of-search-data.html (last visited Nov. 3, 2022).

44. Johana Bhuiyan, *The New Warrant: How US Police Mine Google for Your Location and Search History*, GUARDIAN (Sept. 16, 2021), https://www.theguardian.com/us-news/2021/sep/16/geofence-warrants-reverse-search-warrants-police-google [https://perma.cc/NH93-T4NB].

45. Every six months, Google publishes updated information for the number of requests it receives from government agencies. *Global Requests for User Information*, *supra* note 42.

46. Emil Protalinski, *Chromebooks Outsold Macs Worldwide in 2020, Cutting into Windows Market Share*, GEEKWIRE (Feb. 16, 2021), https://www.geekwire.com/2021/chromebooks-outsold-macs-worldwide-2020-cutting-windows-market-share/ [https://perma.cc/KB23-X8G2].

47. *Law Enforcement Requests Report*, MICROSOFT: CORP. SOC. RESP., https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report [https://perma.cc/R3PB-ETCY].

48. *Internet Health Report 2018*, *supra* note 18. Bing also powers Yahoo Search and other smaller search engines. *Id.*

49. *Government Data Requests*, YAHOO!, https://www.yahooinc.com/transparency/reports/government-data-requests.html [https://perma.cc/6WQD-FV5S].

50. *Id.*

51. *State Laws Related to Digital Privacy*, NAT'L CONF. OF STATE LEGISLATURES,

provides "the right to request a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected,"[52] and the right to "delete any personal information about the consumer."[53] In 2020, California approved Proposition 24.[54] Proposition 24 further limited the amount of information a business can share, such as an individual's geolocation, race, religion, private communications, and more.[55] Two other states have similarly implemented statutes to ensure that companies protect users' personal data. Colorado's law calls on companies to be transparent, minimize data, avoid secondary use, and require data protection assessments.[56] Virginia's law allows individuals to access or delete data, correct any inaccurate data, or opt-out of data used for targeted advertisements.[57]

A. The Keyword Warrant Is a New Tool for Widespread Searches

This Part explores what keyword warrants are and how police departments around the country have taken advantage of Google and other search engines. It then delves into the states' reactions to keyword warrants through legislation.

1. Definition and Known Cases

Keyword warrants require search engines to hand over users' personal information if those users searched for specific terms (or "keywords") on the search engine's website.[58] Keyword warrants do not demand the search history of a specific person, but rather, keyword warrants demand the information of persons who have searched for a single or various keywords. These demands for information are not tied to a crime in terms of location or any other tangible piece of evidence. Instead, keyword warrants suspect individuals who shared a common interest in specific words or addresses.[59] These warrants can ask not only for user identities

---

https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx [https://perma.cc/957B-DD23].

52. California Consumer Privacy Act, Cal. Civ. Code § 1798.100 (2018).

53. *Id.* § 1798.105.

54. Sec. of State of Cal., Proposed Law: The California Privacy Rights Act of 2020 (2020), https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf [https://perma.cc/SU92-L7YX].

55. *Id.*

56. Colorado Privacy Act, COLO. REV. STAT. § 6-1-1301 (2021).

57. Consumer Data Protection Act, VA. CODE ANN. § 59.1-573 (2021).

58. Brewster, *Exclusive: Government Secretly Orders Google*, *supra* note 4.

59. *Id.*

and IP addresses, but also "CookieIDs," which identify whether the same account has conducted searches multiple times within a certain period of time.[60]

In 2019, the federal government tracked down the identities of suspects involved in the trafficking and sexual abuse of a minor.[61] Law enforcement served Google with a search warrant, compelling them to produce the IP addresses and identities of Google accounts who searched specific keywords over the course of sixteen days, including the victim's name, the mother's name, and her address.[62] The public only became aware of this keyword warrant when it was accidentally unsealed and later reported by Forbes.[63]

News outlets have only been recently publicizing keyword warrants, and so far, their use is seemingly limited among law enforcement. According to Richard Salgado, Google's Director of Law Enforcement and Information Security, keyword warrants "represent less than 1% of total warrants and a small fraction of the overall legal demands for user data that [they] . . . receive."[64] Including the 2019 Wisconsin case uncovered by Forbes, a total of eight instances of keyword warrants are known to the public: one in 2017, two in 2018, and five in 2020.[65]

First, in 2017, Google initially fought off an administrative subpoena, but a judge eventually issued a keyword warrant to Google for individuals who had searched a fraud victim's name within the span of a month.[66] The police demanded users' information, including names, addresses, phone numbers, birth dates, social security numbers, payment information, MAC

60. *Id.*

61. *Id.*

62. *Id.*

63. *Id.*

64. Jon Fingas, *Google Is Sharing User Data Tied to Search Keywords with Law Enforcement*, ENGADGET (Oct. 8, 2020), https://www.engadget.com/google-gives-search-keyword-user-data-to-police-144249434.html [https://perma.cc/75NU-X4TX].

65. Andrea O'Sullivan, *The Government's Secret 'Google Search' Warrant Trap*, REASON (Oct. 12, 2021), https://reason.com/2021/10/12/the-governments-secret-google-search-warrant-trap/ [https://perma.cc/WHJ6-9TM7].

66. 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/RH4Y-THJQ]; Application for Search Warrant (Minn. Hennepin Cnty. Ct. Feb. 1, 2017), https://www.documentcloud.org/documents/3519211-Edina-Police-Google-Search-Warrant-Redacted.html (last visited Dec. 8, 2022).

addresses,[67] and IP addresses.[68]

Likewise, in 2018, law enforcement served Microsoft with a warrant for terms entered into Bing search or Bing Maps, specifically addresses in connection with a series of pipe bombings in Texas.[69] The keyword warrant sought the information of individuals who entered any variety of any of those four addresses.[70] The probable cause statement stated that "since the three bombing locations are residences in residential neighborhoods, and not business addresses . . . the pool of individuals searching for these addresses will be relatively small."[71] Law enforcement also served Oath Holdings, parent company of Yahoo, with a warrant for terms entered into Yahoo Search and Yahoo Maps for the same crime.[72] It is difficult to truly tell how many warrants have been issued for other search engines like Bing and Yahoo because there are only keyword warrant numbers for Google.

In 2020, New York law enforcement issued a keyword warrant for anyone who "searched for the address of an arson victim who was a witness in the government's racketeering case against singer R. Kelly"[73] close to the time of the arson.[74] After narrowing the search and identifying a suspect, law enforcement found other searches, such as "the 'detonation properties' of diesel fuel, a list of countries that do not have extradition agreements with the US, and YouTube videos of R. Kelly's alleged victims . . . ."[75] Additionally, in 2020, Forbes found a California warrant

---

67. A MAC Address is a Media Access Control address, which is unique to a device and "generally unchangeable." Raymond Chow, *Why-Spy? An Analysis of Privacy and Geolocation in the Wake of the 2010 Google "Wi-Spy" Controversy*, 39 RUTGERS COMPUT. & TECH. L.J. 56, 63 (2013).

68. Application for Search Warrant, *supra* note 66.

69. Affidavit in Support of Application for Search Warrant at 4, *In re* Search of Info. & Recs. Associated with Microsoft Searches for Various Search Terms that Are Stored at Premises Controlled by Microsoft, No. 1:18-mj-171 (W.D. Tex. Mar. 14, 2018), https://www.documentcloud.org/documents/21077356-microsoft-keyword-warrant-in-austin-2018 (last visited Dec. 8, 2022).

70. *Id.* at 1–2.

71. *Id.* at 10.

72. Affidavit in Support of Application for Search Warrant, *In re* Search of Info. & Recs. Associated with Yahoo Searches for Various Search Terms that Are Stored at Premises Controlled by Oath Holdings Inc., No. 1:18-mj-168 (W.D. Tex. Mar. 14, 2018), https://www.documentcloud.org/documents/21077357-yahoo-keyword-warrant-austin-2018 (last visited Dec. 8, 2022).

73. Brewster, *Exclusive: Government Secretly Orders Google*, *supra* note 4.

74. Affidavit in Support of Application for Search Warrant, *In re* Search of Info. Associated with the Cellular Device Assigned Call No. (229) 418-8231, No. 20-MC-1584 (E.D.N.Y. July 13, 2020), https://www.documentcloud.org/documents/7222789-Another-R-Kelly-Search-Warrant.html (last visited Dec. 8, 2022).

75. Sidney Fussell, *How Your Digital Trails Wind Up in the Police's Hands*, WIRED (Dec. 28,

titled "Search Warrant for Google Accounts Associated with Six Search Terms and Four Search Dates."[76] It is unknown whether or not this is a true keyword warrant, as it is yet to be unsealed.[77]

In October and November 2020, Denver police executed three keyword warrants, searching for identifying information about Google accounts that searched for addresses of where an arson occurred.[78] While the search was meant to only cover the State of Colorado, it proved to be much wider than that.[79] Google refused to comply with the first warrant, because it demanded the full names and addresses of every relevant account.[80] So, police officers issued another warrant. Google also refused to comply with the second keyword warrant because, although it now asked for anonymized information, it also asked for two days of geolocation data from each account.[81] Google finally acquiesced on the government's third attempt, but this time, the government only asked Google for IP addresses.[82] Google provided full IP addresses of sixty-one queries: thirty-eight from Colorado, two from Illinois, and twenty-one from an unknown location.[83] Interestingly, eleven of the queries did not specify the search query at all.[84]

While the public only knows about a limited number of keyword warrants, this does not detract from the potential devastating constitutional violation they may pose. As seen in the small subset of known warrants, thousands or millions of individuals can be affected through a single search. The media has publicized more and more keyword warrants in recent years. Once the public found out about keyword warrants, some states were quick to act through legislation.

2. State Legislative Reaction

In response to the growing number of keyword warrants, New York began to implement legislation against them. On January 6, 2022, the Reverse Location and Reverse Keyword Search Prohibition Act[85] was

---

2020), https://www.wired.com/story/your-digital-trails-polices-hands/ [https://perma.cc/5L3D-2K4Q].

76. Brewster, *Exclusive: Government Secretly Orders Google*, *supra* note 4.

77. *Id.*

78. Motion to Suppress, *supra* note 2, at 7–9.

79. *Id.*

80. *Id.* at 7.

81. *Id.* at 8.

82. *Id.*

83. *Id.* at 9.

84. *Id.*

85. Assemb. B. A84A, 2021–2022 Leg., Reg. Sess. (N.Y. 2022).

reintroduced to the New York State Assembly. In 2020, State Senator Zellnor Myrie and Assemblymember Dan Quart worked with organizations such as the New York Civil Liberties Union and the Surveillance Technology Oversight Project to help get this bill passed.[86] Originally, when Assemblymember Dan Quart and other cosponsors first introduced the bill in April 2020, it only contained a prohibition against the use of geolocation data.[87] The new proposed bill outlaws both geolocation[88] and keyword data in searches "of a group of people who are under no individual suspicion of having committed a crime, but rather are defined by having been at a given location at a given time or searched particular words, phrases, character strings, or websites."[89] Various organizations, such as the New York Civil Liberties Union,[90] Electronic Frontier Foundation,[91] New York City public defense organizations,[92] and even a coalition of major technology companies[93] have actively supported this bill. Some activist organizations have also called upon Google for increased transparency, especially for geofence and keyword warrants.[94]

In Utah, the legislature proposed a similar bill to prohibit reverse

86. Fussell, *An Explosion in Geofence Warrants*, *supra* note 41.

87. Assemb. B. A10246A, 2019–2020 Leg., Reg. Sess. (N.Y. 2020).

88. Further discussion of geolocation or geofence warrants is in section II.B.

89. Assemb. B. A84A, 2021–2022 Leg., Reg. Sess. (N.Y. 2022). Additionally, any evidence acquired as a result of such tactics can be suppressed or excluded by a defendant, and individuals who have been illegally searched this way can sue the government. *Id.* §§ 695.30(1), 695.40(1).

90. NYCLU, *2021-2022 Legislative Memorandum, Prohibits the Use of Reverse Location and Reverse Keyword Searches – A.84 (Quart) / S.296 (Myrie)*, https://www.nyclu.org/sites/default/files/field_documents/2021-legislativememo-reversewarrants.pdf [https://perma.cc/5WU4-3JMN].

91. Hayley Tsukayama, *Standing Up for Privacy in New York State*, ELEC. FRONTIER FOUND. (Jan. 11, 2022), https://www.eff.org/deeplinks/2022/01/standing-privacy-new-york-state [https://perma.cc/AD7Y-VGSV].

92. Letter from Brooklyn Defenders on Legislative Priorities for Criminal Legal System Reform, to Kathy Huchel, Governor, N.Y. State, Andrea Stewart-Cousins, Democratic Leader, N.Y. State Senate, and Carl Heastie, Speaker, N.Y. State Assemb. (Dec. 20, 2021), https://bds.org/assets/files/NYC-Public-Defender-Legislative-Priorities-for-Crim-Legal-System-Reform-2022.pdf [https://perma.cc/9NN8-GWFH].

93. The Reform Government Surveillance coalition, consisting of Amazon, Apple, Dropbox, Evernote, Google, Meta (Facebook), Microsoft, Snap Inc., Twitter, Yahoo!, and Zoom, supports the adoption of A84A. *RGS Urges Adoption of New York's Reverse Location Search Prohibition Act*, REFORM GOV'T SURVEILLANCE (May 5, 2022), https://www.reformgovernmentsurveillance.com/rgs-urges-adoption-of-new-yorks-reverse-location-search-prohibition-act/ [https://perma.cc/Z349-63YL].

94. Letter from S.T.O.P. Coalition to Sundar Pichai, CEO of Google, Re: Need for Improved Transparency on "Geofence" and "Keyword Warrants" (Dec. 8, 2020), https://www.stopspying.org/geofence-letter [https://perma.cc/8FLH-3G6G].

keyword and reverse location data,[95] but the legislature has since deleted references to keyword searches in subsequent revisions to the bill.[96] In addition to dropping keyword searches, Utah's bill also no longer flatly outlaws any reverse location searches, but rather places more restrictions (such as anonymizing personal data) on reverse location searches.[97] Sponsor of the bill, Rep. Ryan Wilcox, stated that "[t]he issues around reverse keyword searches gets us into an area of law that is even more complicated than the location challenges."[98] While New York and Utah are the first states to consider restrictions on keyword warrants, they surely will not be the last, as more and more legal advocates and organizations have questioned the warrants' constitutionality.

II. KEYWORD WARRANTS COMPARED TO GENERAL WARRANTS, THE ENEMY OF THE FOURTH AMENDMENT

Keyword warrants share similarities with general warrants, allowing law enforcement to search any place for any item without specifying either.[99] In the past, general warrants appeared in the American colonies as writs of assistance. In creating the Fourth Amendment, America's founders sought to protect individuals' privacy. Further development of the Fourth Amendment through caselaw has strengthened these privacy rights in some ways and weakened them in others. As time has gone on, law enforcement officials have delved into more contemporary warrants, such as tower dump and geofence warrants, which serve as apt constitutional comparisons to keyword warrants.

---

95. Reverse keyword and reverse location data simply refer to the information retrieved from keyword warrants and geofence warrants or warrants that demand the account information of any devices in a specific location.

96. *Compare* Electronic Keyword and Location Amendments, H.B. 251, 2021 Gen. Sess. (Utah 2021) https://le.utah.gov/~2021/bills/hbillint/HB0251.pdf [https://perma.cc/RN2Q-59XS] (imposing prohibitions on both "reverse-keyword" and "reverse-location" warrants), *with* Electronic Location Amendments, H.B. 251 1st Sub., 2021 Gen. Sess. (Utah 2021), https://le.utah.gov/~2021/bills/hbillamd/HB0251S01.pdf [https://perma.cc/B4SL-4R76] (imposing prohibitions on only "reverse-location" warrants).

97. Electronic Location Amendments, H.B. 251 1st Sub., 2021 Gen. Sess. (Utah 2021), https://le.utah.gov/~2021/bills/hbillamd/HB0251S01.pdf [https://perma.cc/B4SL-4R76].

98. Art Raymond, *Bill Targets How Police Info Showing Where You've Been and What Internet Searches You Make*, DESERETNEWS (Feb. 25, 2021), https://www.deseret.com/utah/2021/2/25/22301633/reverse-location-reverse-keyword-law-enforcement-search-ban-utah-legislature-aclu-personal-privacy [https://perma.cc/X6EN-2RSB].

99. Michael, *supra* note 14, at 909.

A. The Fourth Amendment, a Measure Against Unreasonable Searches in the House and on the Web

At the core of the Fourth Amendment is the protection against suspicionless searches, in which the government could freely search anyone regardless of whether they were suspect to a crime.[100] A historical overview of the Fourth Amendment demonstrates the analogy between these prohibited general searches and modern-day keyword searches. This history then informs the evolution of protecting traditional physical spaces to contemporary digital spaces, as some courts have begun to recognize a reasonable expectation of privacy in internet browsing information.

1. Historical Roots of the Fourth Amendment and Search Warrant Requirements

The Fourth Amendment, like nearly all of the rights enshrined in the Constitution, owes its creation in part to the history of unrestricted power of the British Crown.[101] For example, English custom officers had unlimited power to seize goods that were imported illegally, allowing them to break down doors, search through any room in any house, and forcibly open chests or packages.[102] Within the colonies, customs officers had a similar power, even recruiting ordinary citizens to search and seize through a writ of assistance, which was in effect for the life of the reigning monarch.[103] This was controversial among the colonists. James Otis described the writs as "the worst instrument of arbitrary power" which endangered the liberty of everyone "in the hands of every petty officer."[104] Inspired by Otis's passionate arguments, along with other misuses of search and seizure power across the colonies and England,[105] John Adams drafted Article 14 of the Massachusetts Declaration of Rights,[106] the

100. City of Indianapolis v. Edmond, 531 U.S. 32, 37 (2000) ("A search or seizure is ordinarily unreasonable in the absence of individualized suspicion of wrongdoing.").

101. *See* Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1196–1207 (2016) (describing a series of cases rejecting general warrants which allowed for "indiscriminate search and seizure").

102. Michael, *supra* note 14, at 907.

103. *Id.* at 907–08.

104. Stanford v. Texas, 379 U.S. 476, 481 (1965).

105. Carpenter v. United States, __ U.S. __, 138 S. Ct. 2206, 2213 (2018); *Stanford*, 379 U.S. at 482 ("[W]hile the Fourth Amendment was most immediately the product of contemporary revulsion against a regime of writs of assistance, its roots go far deeper. Its adoption in the Constitution of this new Nation reflected the culmination in England a few years earlier of a struggle against oppression which had endured for centuries.").

106. Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979, 981 (2011).

provision serving as the blueprint for the Fourth Amendment.[107]

In 1791, the states ratified the Fourth Amendment, drafted by James Madison.[108] It declared:

> 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.[109]

The Fourth Amendment begins with an emphasis on "the rights of the people," and dual rights in both the security of one's person and the security of one's property.[110] The language above resulted from a lively debate, incorporating concerns about general warrants, such as the writs of assistance, and "ensuring that the rights of the people would be secure against government overreach."[111] General warrants are warrants that only specify an offense, leaving it up to law enforcement officials to decide as to which persons should be arrested and seized.[112] General warrants have historically been banned because of this lack of particularity.[113]

In subsequent decades, litigation and legislation both expanded and contracted the meaning of Madison's words. Under *Katz v. United States*,[114] when the government invades the privacy on which an individual "justifiably relied,"[115] it is a search that triggers the protections of the Fourth Amendment, requiring a warrant.[116] For example, a person standing in an open field does not have a reasonable expectation of privacy because they are "accessible to the public and the police in ways that a home, office, or commercial structure would not be."[117] Justice Harlan, concurring in *Katz*, proposed that an individual must have a

---

107. *Id.* at 982, 1052.

108. Donohue, *supra* note 101, at 1299, 1305.

109. U.S. CONST. amend. IV.

110. Donohue, *supra* note 101, at 1299.

111. *Id.* at 1284.

112. Scott E. Sundby, *Protecting the Citizen "Whilst He Is Quiet": Suspicionless Searches, "Special Needs" and General Warrants*, 74 MISS. L.J. 501, 505–06 (2004).

113. *Id.* at 508.

114. 389 U.S. 347 (1967).

115. *Id.* at 353 ("The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment.").

116. *Id.* at 357. If an individual wants something preserved as private and their expectation of privacy is reasonable, "official intrusion into that sphere" is a search. Carpenter v. United States, 585 U.S. __, 138 S. Ct. 2206, 2213 (2018).

117. Oliver v. United States, 466 U.S. 170, 171 (1984).

"reasonable expectation of privacy" in order to be protected under the Fourth Amendment,[118] resulting in a two-part test[119] that has subsequently been used by the courts.[120] To have a reasonable expectation of privacy in an area, the individual must exhibit an actual subjective expectation of privacy and that expectation must be one society is prepared to recognize as reasonable.[121] This means that it is not enough for one to think one is in a private space, but rather, others must generally believe that one has privacy there as well.[122] If the area to be searched does meet both of these prongs, then the government must retrieve a warrant to enter the premises.[123]

The requirements to receive a warrant under the Fourth Amendment are strict. A warrant must be: (1) built upon probable cause; (2) supported by oath, usually from a magistrate judge; and (3) must particularly describe the place to be searched or the persons or things to be seized.[124] A magistrate judge will determine a warrant has probable cause if there is a "fair probability" that evidence of a crime will be found in a certain area.[125]

The third requirement, particularity, is integral to the constitutionality of the warrant.[126] In order for a warrant to meet the particularity requirement, the warrant must include a description that is "such that the officer with a search warrant can, with reasonable effort ascertain and identify the place intended."[127] A warrant that is sufficiently particularized is specifically tailored to a place.[128] If the police are looking for drugs, they cannot issue a warrant for both a suspect's home and their place of work, as that is not narrow or particular enough. The police must have information as to where it is more likely to find the drugs and issue a warrant for that place within a reasonable time.[129] Even a search warrant for digital evidence must particularize the digital evidence that the

118. *Katz*, 389 U.S. at 360.

119. *Id.* at 361.

120. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 742–44 (1979) (holding that one cannot have a reasonable expectation of privacy in a pen registry because people do not have an expectation that the numbers they dial on the telephone will be kept private).

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

122. *Id.*

123. *See* U.S. CONST. amend. IV.

124. *Id.*

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

126. Groh v. Ramirez, 540 U.S. 551, 559 (2004).

127. Steele v. United States, 267 U.S. 498, 503 (1925).

128. *Id.*

129. *See* Adam M. Gershowitz, *The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, 69 VAND. L. REV. 585, 598 (2016).

government is seizing based on the crimes for which there is probable cause.[130] This particularity limits the scope of searches both spatially and temporally, and it is this requirement that hearkens back to the abuse of authority that the state had exercised on the colonists using general search warrants.

2. Applying the Fourth Amendment in the Digital Age: Privacy in Internet Browsing History

Today, for the Fourth Amendment to apply to internet browsing history, internet users must have a reasonable expectation of privacy in search history. Privacy in an area does not always have to be a physically bounded space, like a house or a suitcase. For instance, the Sixth Circuit held that there was a reasonable expectation of privacy in the content of emails[131] and cell phone location records.[132] Further, several circuit courts held that there is a reasonable expectation of privacy in internet browsing data.[133] For example, in considering intrusion upon seclusion and invasion of privacy civil actions under California law, the Ninth Circuit held that social media users plausibly alleged a reasonable expectation of privacy in internet browsing data and history.[134] The Third Circuit found that while a "sophisticated internet user" may know that their URL information was sent to Google, they "would also reasonably expect" that an activated cookie blocker, which prevents advertising companies from tracking and monitoring an individual's internet activity, would secure their information.[135]

Previously, courts made the argument that there is no expectation of

---

130. Kaitlyn R. O'Leary, Note, *What the Founders Did Not See Coming: The Fourth Amendment, Digital Evidence, and the Plain View Doctrine*, 46 SUFFOLK U. L. REV. 211, 221–22 (2013).

131. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding that there was a reasonable expectation of privacy in emails held by an internet service provider, but because government agents relied in good faith on provisions of the Stored Communications Act, the evidence in the emails could not be excluded).

132. Carpenter v. United States, 585 U.S. __, 138 S. Ct. 2206, 2219 (2018) ("[W]hen the Government accessed [cell site location information] from the wireless carriers, it invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements.").

133. *See In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589 (9th Cir. 2020); *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125 (3d Cir. 2015).

134. *In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589.

135. *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d at 151 ("[A] sophisticated internet user may well have known that, in browsing the internet, her URL information was sent to Google. But such a user would also reasonably expect that her activated cookie blocker meant her URL queries would not be associated with each other due to cookies. As the activated cookie blocker equates, in our view, to an express, clearly communicated denial of consent for installation of cookies, we find Google 'intru[ded] upon reasonable expectations of privacy.'" (quoting Hernandez v. Hillsides, Inc., 211 P.3d 1063, 1074 (Cal. 2009))); Foley, *supra* note 40, at 462.

privacy in search history because the data is held by third parties, and is therefore not constitutionally protected, as the user's own volition shares that information.[136] Pursuant to *Katz v. United States*, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not subject to Fourth Amendment protection."[137] Under *Smith v. Maryland*,[138] the Court found that an individual lacks a reasonable expectation of privacy in information they give to third parties.[139] However, *Katz* asserted that a narrow reading of the Fourth Amendment, one that precludes the privacy of a shut telephone booth, "ignore[s] the vital role that the public telephone has come to play in private communication."[140]

Similar to the court's sentiment about the public telephone in *Katz*, disclosing information to search engines "is practically inevitable in order to participate in modern life."[141] Because individuals must give away their personal information to access such essential technology and they believe that disclosure remains private, they still retain their reasonable expectation of privacy when giving their information to search engine third parties.[142] Justice Sonia Sotomayor echoes this sentiment within her concurrence in *United States v. Jones*,[143] where she questions the third party doctrine in the digital age, believing that not all information voluntarily disclosed should preclude Fourth Amendment protections.[144]

The Supreme Court debated how to anticipate technological advancement to prevent the erosion of the reasonable expectation of privacy. If surveillance technology becomes more widespread, it becomes less reasonable for individuals to believe that they are in a private space. In *Kyllo v. United States*,[145] the Court confronts the question of "what limits there are upon [the] power of technology to shrink the realm of guaranteed privacy."[146] *Kyllo* turned on whether the technology used by

136. Foley, *supra* note 40, at 464.

137. Katz v. United States, 389 U.S. 347, 351 (1967).

138. 442 U.S. 735 (1979).

139. *Id.* at 743–44.

140. *Katz*, 389 U.S. at 352.

141. Foley, *supra* note 40, at 465.

142. *Id.* at 468.

143. 565 U.S. 400 (2012).

144. *Id.* at 417–18 (Sotomayor, J., concurring) ("This approach 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. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.")

145. 533 U.S. 27 (2001).

146. *Id.* at 34.

the police was "in general public use."[147] If the police use a device not in general public use, "the surveillance is a 'search'" under the Fourth Amendment "and is presumptively unreasonable without a warrant."[148]

Statutory protections on information also inform what people reasonably expect to be private. Currently, there are statutory protections for online information under the Electronic Communications Act (ECPA),[149] but it is contested whether search queries and URLs are protected.[150] The ECPA protects "contents of any wire, oral, or electronic communication,"[151] which is defined as information concerning "the substance, purport, or meaning of that communication."[152] A Massachusetts district court held that search terms can be considered as content because "the 'substance' and 'meaning' of the communication is that the user is conducting a search for information on a particular topic."[153] This court's reasoning provides evidence of the fact that people could reasonably expect privacy in search queries. If the legislature or the judiciary deem search queries are content information protected under the ECPA, then courts would have a rational basis in arguing that society believes there is a reasonable expectation of privacy in search queries.

B. Dragnet Search Analogies to Tower Dump and Geofence Warrants

Today, general warrants are considered patently unconstitutional, and yet, echoes of general warrants and widespread, unrestricted searches can be seen in the new technology law enforcement departments around the nation choose to employ. This is dragnet policing, a practice that sweeps up innocent civilians in a search in order to find the identities of suspects. Because there is little information and litigation on keyword warrants and there are only eight keyword warrants known to the public, analyzing the treatment of tower dump and geofence warrants can aide us in determining both the constitutionality and practicability of keyword warrants.

Keyword warrants share some things in common with cell tower dump warrants. Cell tower dump warrants review cell site location data for any

147. *Id.* at 28.

148. *Id.* at 40.

149. 18 U.S.C. § 2701.

150. Foley, *supra* note 40, at 458.

151. 18 U.S.C. § 2511(1)(c)–(e).

152. *Id.* § 2510(8).

153. *In re* Application of U.S. for an Ord. Authorizing Use of a Pen Reg. & Trap On (XXX) Internet Serv. Acct./User Name, (xxxxxxxx@xxx.com), 396 F. Supp. 2d 45, 49 (D. Mass. 2005).

users in an area. Generally, long-term historical cell site location information constitutes a Fourth Amendment search.[154] Under the Supreme Court's current standard in *Carpenter v. United States*,[155] individuals usually have a reasonable expectation of privacy for at most, a seven-day period.[156] Tower dumps are distinct from traditional cell site location tracking of a single person, as these methods collect cell site location information from thousands of people and span several hours or minutes.[157]

Most lower courts ruled that there is no reasonable expectation of privacy in cell tower dump location information, but it is important to note that many of these decisions came before the Supreme Court's latest ruling on cell site location information.[158] Post-*Carpenter*, the Second and Ninth Circuits followed the Supreme Court and held that there is a reasonable expectation of privacy in cell site data.[159]

Google location history is even more precise and powerful than tower dump information.[160] Officers use reverse location warrants, which request unique Google user information within the limited time period and area (or "geofence") the crime was committed.[161] For example, in response to a murder at a park, the government can compel Google to show them the users who have passed by or through the park within the time period that the murder occurred. Once Google provides this information, the government reviews it and produces a list of devices it wants additional information for.[162] Google must produce the identifying information for the requested devices.[163] These geofence warrants have

---

154. *See* Carpenter v. United States, 585 U.S. __, 138 S. Ct. 2206 (2018).

155. 585 U.S. __, 138 S. Ct. 2206 (2018). In *Carpenter*, the government obtained a warrant for the defendant's cell phone search histories, specifically the location of incoming and outgoing calls when the crime occurred, providing the government with around 101 data points throughout the day. *Id.* at 2212.

156. *Id.* at 2217 n.3.

157. Emma Lux, Comment, *Privacy in the Dumps: Analyzing Cell Tower Dumps Under the Fourth Amendment*, 57 AM. CRIM. L. REV. ONLINE 109, 109–10 (2020).

158. *Id.* at 110; *see, e.g.*, *In re* U.S. for Hist. Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (holding that cell site data should not be considered protected under the Fourth Amendment, but rather should be analyzed as business records under the Stored Communications Act).

159. United States v. Chambers, 751 F. App'x 44, 45 (2d Cir. 2018); United States v. Elmore, 917 F.3d 1068, 1073 (9th Cir. 2019).

160. Brief of Google LLC in Supp. of Neither Party Concerning Def.'s Mot. to Supp. Evid. from a "Geofence" Gen. Warrant, ECF No. 29, at 10, United States v. Chatrie, __ F.Supp.3d. __, 2022 WL 628905 (E.D. Va. 2019) (No. 3:19-cr-00130-MHL) [hereinafter Google Amicus Brief].

161. *In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345, 351 (N.D. Ill. 2020).

162. *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2509 (2021).

163. *Id.* at 2513–15.

been used to locate a variety of individuals, ranging from a suspect of a Virginia bank robbery[164] to a group of violent Proud Boys in Manhattan.[165] Caleb Kenyon, a defense lawyer who represented a client who was the subject of a geofence warrant, described them as "true digital warrant[s], without any ties or connections or tethers to the physical world."[166]

Many judges ruled that geofence warrants that are supported by probable cause and are particular in time, location, and scope are constitutional,[167] despite grounds of probable cause often being solely based on a user's device being present near the scene.[168] However, various magistrate judges have held that geofence warrants violate the Fourth Amendment.[169] An Illinois magistrate judge held that a geofence warrant did not meet the particularity requirement because it did not list the people "whose location information the government will obtain from Google" and "puts no limit on the government's discretion to select the device IDs from which it may then derive identifying subscriber information."[170]

Furthermore, in *United States v. Chatrie*,[171] a Virginia district court

---

164. Deanna Paul, *Alleged Bank Robber Accuses Police of Illegally Using Google Location Data to Catch Him*, WASH. POST (Nov. 21, 2019), https://www.washingtonpost.com/technology/2019/11/21/bank-robber-accuses-police-illegally-using-google-location-data-catch-him/ [https://perma.cc/QB4Y-4Y5Z].

165. Albert Fox Cahn, *Manhattan DA Made Google Give Up Information on Everyone in Area as They Hunted for Antifa*, DAILY BEAST (Aug. 15, 2019), https://www.thedailybeast.com/manhattan-da-cy-vance-made-google-give-up-info-on-everyone-in-area-in-hunt-for-antifa-after-proud-boys-fight/ [https://perma.cc/KXJ4-7FSY].

166. Bhuiyan, *supra* note 44.

167. *Geofence Warrants and the Fourth Amendment*, *supra* note 162, at 2509.

168. *See* Search Warrant (Minn. Hennepin Cnty. Ct. Aug. 11, 2020), https://www.documentcloud.org/documents/20473889-minneapolis-police-searchgeolocation-warrant (last visited Dec. 8, 2022).

169. Jennifer Lynch & Nathaniel Sobel, *New Federal Court Rulings Find Geofence Warrants Unconstitutional*, ELEC. FRONTIER FOUND. (Aug. 31, 2020), https://www.eff.org/deeplinks/2020/08/new-federal-court-rulings-find-geofence-warrants-unconstitutional-0 [https://perma.cc/BT2P-74NK]; *In re* Search of Info. Stored at Premises Controlled by Google, No. 20 M 297 (D.E. 4) (N.D. Ill. July 8, 2020), https://www.eff.org/files/2020/08/31/order_20_m_297.pdf [https://perma.cc/KA8E-GY2E]; *In re* Search Info. Stored at Premises Controlled by Google, No. 20 M 392 (N.D. Ill. July 24, 2020), https://www.eff.org/document/re-search-information-stored-premises-controlled-google-no-20-m-392-nd-ill-july-24-2020 [https://perma.cc/264S-AUTY]; *In re* Search of Info. Stored at Premises Controlled by Google, No. 20 M 392, 2020 U.S. Dist. LEXIS 152712 (N.D. Ill. Aug. 24, 2020), https://www.eff.org/files/2020/08/31/13_20-mc-00392.pdf [https://perma.cc/F859-646H]; *In re* Search of Info. Stored at the Premises Controlled by Google, No. 21-MJ-5064 (D. Kan. June 4, 2021), https://www.eff.org/document/matter-search-information-stored-premises-controlled-google-no-21-mj-5064-d-kan-june-4-2021 [https://perma.cc/3PUH-2CHL].

170. *In re* Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 754 (N.D. Ill. 2020).

171. No. 3:19CR130, 2022 WL 628905 (E.D. Va. Mar. 3, 2022).

judge deemed that a geofence warrant was invalid because it lacked particularized probable cause for each of the nineteen users caught in the geofence area.[172] Even though the government then narrows the number of users after the initial geofence search, the warrant does not contain "language objectively identifying which accounts for which officers would obtain further identifying information" or "provide objective guardrails by which officers could determine which accounts would be subject to further scrutiny."[173] The *Chatrie* court also states that it is "disturbed that individuals other than criminal defendants caught within expansive geofences may have no functional way to assert their own privacy rights."[174] The fact that one individual's privacy rights are impacted by a search is not uncommon. While the geofence warrant in *Chatrie* involved nineteen devices,[175] one of the biggest geofence warrants was for a series of arsons in Milwaukee which swept up 1,494 devices.[176]

Geofence warrants are surrounded by secrecy and limited oversight.[177] The issue is that the court usually seals most geofence warrants that are issued, even though there is no act or regulation requiring so.[178] It is important to note that these warrants, like many other warrants, are usually insufficiently detailed and may be approved in mere minutes by a judge.[179] Google sometimes notifies users when their data turns up in a warrant, including one innocent user who became a suspect in a Gainesville burglary through a geofence warrant.[180] Geofence warrants have increased in recent years, yet geofence warrants "often do not lead to catching perpetrators."[181] In 2018, Jorge Molina was wrongfully

---

172. *Id.* at *18 (holding even though the geofence warrant was held to be constitutionally defective, the motion to suppress was denied because the warrant was deemed in good faith "in light of rapidly advancing technology and lack of judicial guidance"). *Id.* at *27.

173. *Id.* at *25.

174. *Id.* at *17.

175. *Id.*

176. Thomas Brewster, *Google Hands Feds 1,500 Phone Locations in Unprecedented 'Geofence' Search*, FORBES (Dec. 11, 2019), https://www.forbes.com/sites/thomasbrewster/2019/12/11/google-gives-feds-1500-leads-to-arsonist-smartphones-in-unprecedented-geofence-search/?sh=7ff7a08c27dc [https://perma.cc/9SNN-7W77].

177. *Geofence Warrants and the Fourth Amendment*, *supra* note 162.

178. *Id.* at 2514.

179. *Id.*

180. Jon Schuppe, *Google Tracked His Bike Ride Past a Burglarized Home. That Made Him a Suspect.*, NBC NEWS (Mar. 7, 2020), https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761 [https://perma.cc/8SZN-CEHF].

181. *Geofence Warrants and the Fourth Amendment*, *supra* note 162, at 2509. Phoenix police wrongly arrested a man they found through a geofence warrant that requested user information on all devices recorded near a murder. Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet*

arrested for murder based on location data history from a geofence warrant.[182] Requests for geofence warrants to Google increased 1,500% from 2017 to 2018 and 500% from 2018 to 2019.[183] In fact, as of 2020, geofence warrants consist of more than 25% of all warrants Google receives in the United States.[184] Two bills have been introduced to enforce restrictions on geofence searches.[185]

From the American colonial era to today's technological age, law enforcement has always sought to take advantage of the tools at their disposal. Keyword warrants are no exception. Search engines store personal data and constantly add more data as technology becomes more pervasive.[186] This allows the power of keyword warrants to grow over time. The question is whether this invasive investigation tactic is constitutional under the Fourth Amendment.

III. PROTECTING USERS FROM INVASIVE GOVERNMENT KEYWORD SEARCHES

This Comment proposes calls to action for the courts, technology companies, and the legislature. Millions of Americans have conducted at least one Google search, and that simple search could get them swept up in an investigation they have no knowledge of and never will. By requesting a warrant, the government believes they can access this type of private information and catch a perpetrator based on what the perpetrator happened to think of and search for. However, a warrant is not enough. As argued in Part III, the government cannot sufficiently particularize keyword warrants of this nature to meet the warrant requirements of the Fourth Amendment. Courts must strike down keyword warrants.

---

for the Police., N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html [https://perma.cc/53H5-AHHK].

182. Meg O'Connor, *Avondale Man Sues After Google Data Leads Wrongful Arrest for Murder*, PHOENIX NEW TIMES (Jan. 16, 2020), https://www.phoenixnewtimes.com/news/google-geofence-location-data-avondale-wrongful-arrest-molina-gaeta-11426374 [https://perma.cc/ERP3-AVTQ].

183. Google Amicus Brief, *supra* note 160, at 3.

184. *Supplemental Information on Geofence Warrants in the United States*, GOOGLE, https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf [https://perma.cc/V6FW-45HR].

185. H.B. 251, 2021 Leg., Gen. Sess. (Utah 2021); Assemb. B. A84A, 2021-2022 Leg., Reg. Sess. (N.Y. 2022).

186. Kristen Purcell, Joanna Brenner & Lee Reinie, *Search Engine Use 2012*, PEW RSCH. CTR (Mar. 9, 2012), https://www.pewresearch.org/internet/2012/03/09/main-findings-11/ [https://perma.cc/KVA3-3MM4] ("A February 2012 Pew Internet survey finds that 91% of online adults use search engines to find information on the web . . . . On any given day online, 59% of those using the Internet use search engines. In 2004 that figure stood at just 30% of internet users.").

In addition to proposing that courts must protect user privacy by striking down keyword warrants as unconstitutional, this Comment argues that technology companies and the legislature must also follow suit. Law enforcement will continue to conduct these searches. Until these searches are outlawed, technology companies must ensure that they are protecting their users by anonymizing their data. The individual has very little choice in providing their data to companies, so companies have a responsibility to safeguard users' privacy. The legislature must implement legislation that halts the encroachment of individual privacy rights. The advent of the keyword warrant signals new kinds of searches and surveillance tools that the framers of the Constitution could not even dream of. The legislature can provide strong protections for user personal information.

A. Keyword Warrants Are a Modern Form of General Warrants and Should Be Outlawed

Under *Katz v. United States*, an individual must have a reasonable expectation of privacy for a search to fall under the protections of the Fourth Amendment.[187] If individuals have a reasonable expectation of privacy in search history, government requests for user information based on search history are searches under the Fourth Amendment.[188] The practice of keyword warrants already assumes that requesting browsing information is a Fourth Amendment regulated search that requires a warrant. Because warrants are usually only issued for Fourth Amendment protected areas, the government already concedes that there is a reasonable expectation of privacy in internet browsing history. The Ninth Circuit and Third Circuit agree with this.[189] Other courts should as well.

Despite individuals providing this information to search engines, users still reasonably believe that they are the only ones who can see their browsing history and that it remains private.[190] Internet browsing has become so integrated into society, and users must communicate this information to search engines in order to access internet browsing privileges. Many users have never read any search engine's privacy policy.[191] Many users do not know or cannot delete their search history or access other, less popular alternatives.[192] As a result, users do not freely

187. Katz v. United States, 389 U.S. 347, 357 (1967).

188. Foley, *supra* note 40, at 468.

189. *In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589 (9th Cir. 2020); *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 151 (3d Cir. 2015).

190. *See supra* section II.A.2; Foley, *supra* note 40, at 468.

191. Litman-Navarro, *supra* note 34.

192. Park, *supra* note 33, at 218.

consent to providing this information, but rather, they provide it as part of a process to access an essential, everyday tool.

Keyword warrants are general warrants in terms of scope and invasiveness. Under the Fourth Amendment, warrants must be particularized so that officers can be bound to searching a single place, as officers already have a suspect.[193] However, officers cannot particularize keyword warrants because the context behind a search is not necessarily connected to a specific perpetrator. The government is essentially "fishing" for suspects, taking a fishing net, throwing it into the ocean, and hoping they catch the perpetrator. In this sense, we can draw historical comparisons to writs of assistance, the general warrants allowing the government to search people without individualized suspicion.[194] This was the injustice that the framers of the constitution sought to avoid in requiring Fourth Amendment particularization. This was the injustice that the court in *Steele v. United States*[195] sought to avoid by necessitating law enforcement tailor a warrant to a specific place based on the crime.

Additionally, keyword warrants are usually bound by time, but they are not bound sufficiently by place. For example, one keyword warrant was bounded within an entire city of thousands and thousands of individuals.[196] The government does not even know the number of individuals they swept up by a warrant until after they receive the information from the third-party technology company. Law enforcement can go to a single company, Google, and receive information for a multitude of individuals because it is the most popular and the most convenient option. A single search can sweep up thousands of innocent people, which is the very act that the creators of the Fourth Amendment were trying to prevent. While keyword warrants are rare, this does not diminish the danger of these widespread and unregulated searches.

Although keyword warrants share similarities with geofence and tower dump warrants, keyword warrants deal with different types of data that could be potentially more intrusive. Cell tower dumps and geofence warrants reveal a physical, objective location that, in certain cases, the Supreme Court has found constitutional because individuals are not likely to have a reasonable expectation for privacy in physical location data. For example, geofence warrants reasonably bounded by time and place are constitutional because of the precision with which Google can pinpoint

193. Steele v. United States, 267 U.S. 498, 503 (1925).

194. *See supra* section II.A.1.

195. 267 U.S. 498 (1925).

196. O'Sullivan, *supra* note 65.

users at a single place and time.[197] In contrast, keyword warrants delve into minds, rather than anything physical or tangible. Keyword warrants do not provide evidence of an individual physically being at or near a crime scene.[198] Rather, individuals are implicated based on what they happened to search during a certain period.[199] Individuals could reasonably expect their location and movements to be known by the public, but this Comment argues that individuals have a reasonable expectation of privacy in their search history, which is not known to the public.

Even if keyword warrants may be able to pinpoint a time, generally, the only other connection to the user is the content of the search query.[200] The information provided by a keyword warrant is not as precise as pinpointing a person at the spot of a crime.[201] Rather, a search query can be made for nearly any reason and should not be sufficient to sweep up users in a criminal search. In fact, if courts follow the standard set in *United States v. Chatrie*, then the government needs particularized probable cause for each individual user or device swept up in the search.[202] That is nearly impossible. The Virginia district court judge in *Chatrie* required probable cause for each of the nineteen users affected,[203] so how can the government acquire probable cause for the potential hundreds of individuals swept up in a keyword search? Keyword warrants reach far beyond the permissible scope of cell tower dumps or geofence warrants.

An officer with a keyword warrant cannot "ascertain and identify the place intended"[204] because the scope is unknowable until the search is already complete. Additionally, the search itself is predicated on sifting through intimate user information,[205] rather than the objective location of a user, as seen in geofence warrants.[206] Therefore, keyword warrants cannot be sufficiently particularized and courts must strike them down as unconstitutional under the Fourth Amendment.

---

197. *Geofence Warrants and the Fourth Amendment*, *supra* note 162, at 2509.

198. Brewster, *supra* note 4.

199. *Id.*

200. *Id.*

201. *Id.*

202. United States v. Chatrie, No. 3:19CR130, 2022 WL 628905, at *18 (E.D. Va. Mar. 3, 2022).

203. *Id.*

204. Steele v. United States, 267 U.S. 498, 503 (1925).

205. *See* Application for Search Warrant, *supra* note 66.

206. *See In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345, 351 (N.D. Ill. 2020).

B. Technology Companies Have a Social Responsibility to Mitigate the Harm

Technology companies must take more steps to protect user information from third parties, both internally, within their own infrastructure, and externally, through fighting outside requests. Technology companies are caught between a rock and a hard place. Technology companies promise to secure user privacy, yet they must break that promise when the government comes knocking. Considering the incredible amount of information that these companies store and how much users place their trust in them, search engine companies need to engage in proactive practices that best ensure the protection of intimate user information.

This Comment proposes three ways that companies may mitigate the harm, providing less user personal information to third parties or preventing searches altogether: (1) allow users to and inform users how to permanently delete their information; (2) provide anonymous or guest browsing; and (3) fight against keyword warrants when requested by the government and provide more transparency for the public.

First, companies must allow users to permanently delete their search history from every log and internal database.[207] Currently, Google does not permanently delete user search history even if users attempt to delete their histories on Google's platform, as Google "still maintains records about the way you used its web browser related to the deleted data."[208] Google keeps this data to target users with individualized advertisements, and even when it is deleted by the user, Google keeps information for audits and internal uses.[209] Although Google now auto-deletes search history after a certain period, this is only a feature available for new users, who have created an account in the past few years.[210] Internet browsing history is content created by a user, so the user should be able to delete that content upon request. Companies must at least sever the tie between the user and the search, anonymizing the identity of the person who made the search query if Google must keep this information for their own records.

---

207. Alix Lagone, *Even If You Clear Your History, Google Has a Record of All of Your Search Activity — Here's How to Delete It*, BUS. INSIDER (Apr. 16, 2018), https://www.businessinsider.com/even-if-you-cleared-your-history-google-records-your-search-activity-2018-4 [https://perma.cc/U8GL-8XRS].

208. *Id.*

209. *Id.*

210. Alfred Ng & Richard Nieva, *Google Makes Auto-Deleting Data the Default for New Accounts*, CNET (May 27, 2020), https://www.cnet.com/news/google-sued-by-arizona-over-location-data-and-alleged-consumer-fraud/ [https://perma.cc/Z2VJ-2YUQ].

Second, companies must also provide accessible avenues for truly anonymous browsing, allowing users to input a search query, either without that query being logged into the search engine's system or by being immediately and permanently deleted after being processed.[211] Google Chrome, Google's internet browser, has an "incognito" service which purports to keep a user's activities private, but it does not keep them completely anonymous. While incognito mode prevents Google from saving data onto a user's account and browsing history, it does not prevent Google from exchanging information to the website the user is interacting with.[212]

Third, companies must actively push against keyword warrants and future versions of general warrants. Users are severely disadvantaged as no party may ever alert them when their user information is divulged, so companies have a duty to protect their users. Google has been attempting to do this when they reject administrative subpoenas or warrants requesting keyword information or narrow those requests, but Google still hands over information in a majority of cases.[213] Companies can file amicus briefs in support of users or at least, briefs that provide accurate, transparent information on its search engine, like Google's amicus brief in response to litigation against a geofence warrant in *Chatrie*.[214] Google not only filed a brief in *Chatrie*, but it also provided "in-person testimony regarding the company's acquisition, retention, and use of users' location data" and various employees submitted declarations.[215] Companies can also direct support to activist organizations, such as the Electronic Frontier Foundation, or legislation, like New York's new keyword warrant bill.

C. The Legislature Should Heed the Technological Encroachment on Users' Privacy Rights

While courts need to guide Fourth Amendment jurisprudence needs in a different direction to anticipate technological advances, the legislature is the ideal body to make lasting changes. As Justice Scalia stated in *Kyllo v. United States*, "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely

211. Lagone, *supra* note 207.

212. *How Chrome Incognito Keeps Your Browsing Private*, GOOGLE CHROME HELP, https://support.google.com/chrome/answer/9845881?hl=en#zippy=%2Chow-incognito-mode-works%2Chow-incognito-mode-protects-your-privacy [https://perma.cc/Q388-C9UJ].

213. *Global Requests for User Information*, *supra* note 42.

214. Google Amicus Brief, *supra* note 160, at 8, 10.

215. United States v. Chatrie, No. 3:19CR130, 2022 WL 628905, at *2 (E.D. Va. Mar. 3, 2022).

unaffected by the advance of technology."[216] Many state courts have already construed their state constitutions' search and seizure provisions to be more protective than the U.S. Constitution.[217] Keyword warrants are simply one example of dragnet policing routing into dangerous territory. However, the legislature is in the optimal position to protect internet users, whether it chooses to implement procedures that prohibit government keyword searches or to go straight to the source and require companies to allow and inform consumers how to control their internet footprint. Most Americans are concerned about government collection of information on Google,[218] but many have not taken any steps to better protect their privacy.[219] Revelations about how much information Google keeps on users regardless of their settings shows that any steps users could take may be in vain.[220]

While users should be more informed and conscious about their internet footprint, this is simply not a feasible reality for all communities. Internet access is a privilege. It is not the individual's responsibility to tread carefully when they have a right to be safe in their persons and effects. Groups that are statistically less likely to have digital literacy, such as historically marginalized communities and communities with older or poorer populations,[221] are more likely to be swept up in these dragnet searches. Digital literacy refers to the ability to adequately operate

---

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

217. Michael J. Gorman, *Survey: State Search and Seizure Analogs*, 77 MISS. L.J. 417 (2007); *see* Sue Davis & Taunya Lovell Banks, *State Constitutions, Freedom of Expression, and Search and Seizure: Prospects for State Court Reincarnation*, 17 PUBLIUS 13, 14 (1987) ("[T]he U.S. Supreme Court has rendered restrictive decisions in each area [access to private property for expression and fruits of illegal searches and seizures] and has consequently given state courts the opportunity to use their own constitutions to provide greater protection of the rights involved in each of these areas."); *see also* William J. Brennan, Jr., *State Constitutions and the Protection of Individual Rights*, 90 HARV. L. REV. 489, 491 (1977) (emphasizing that state constitutions are required to fully realize our individual rights).

218. Around 69% of surveyed Americans are concerned about the collection and use of personal information by websites like Google, Amazon, or eBay. Todd Lindeman, *The Public Worries About Surveillance . . .*, WASH. POST (Dec. 21, 2013), https://www.washingtonpost.com/business/economy/the-public-worries-about-surveillance-but-few-take-steps-to-protect-their-privacy/2013/12/21/529c296a-6ab0-11e3-8b5b-a77187b716a3_graphic.html [https://perma.cc/LD85-DGJB]. Additionally, 66% of Americans do not want advertisements tailored to their interests. Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley & Michael Hennessy, *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It*, N.Y. TIMES 3 (Sept. 2009), https://www.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf [https://perma.cc/AEE4-E42A].

219. Lindeman, *supra* note 218.

220. *Supra* section I.A.

221. Mamedova & Pawloski, *supra* note 31, at 5.

a computer and navigate the internet.[222] Without this knowledge to evaluate how much trust to put into the internet and internet searches, low digital literacy rates put already vulnerable groups at greater risk for exploitation. A person's race, religion, ethnicity, and immigration status shape their contacts with the police,[223] and technology further exacerbates that tension by granting police access to mass surveillance.[224] Because these "communities are over-surveilled, they tend to be over-policed, resulting in inflated arrest rates and increased exposure to incidents of police violence."[225] This is why legislators need to take action and protect vulnerable communities from suffering even more harm.

Without adequate legislation pushing privacy rights in a more protective direction, keyword searches will likely become more pervasive. Keyword searches are an easy tool to fish out potential suspects, but the easiest way is not always the right way. Bills are currently in motion in the state legislatures, such as New York's Reverse Location and Reverse Keyword Search Prohibition Act[226] or Utah's Electronic Location Amendments,[227] that are combatting these issues. Other states and Congress must follow suit. The courts can only do so much. Due to the secretive nature of keyword warrants and the fact that many individuals do not even know if their rights have been violated,[228] it will be rare to see a keyword warrant appealed, much less appealed to a state or the U.S. Supreme Court. In order to have truly robust protections, a statute must prevent law enforcement from implementing these kinds of invasive tactics.

---

222. Digital illiteracy is classified by the Program for the International Assessment of Adult Competencies as adults "who reported no computer use, who were unwilling to take the assessment on the computer, or who failed the basic computer test." *Id.* at 2.

223. Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 347 (4th Cir. 2021) (quoting Barton Gellman & Sam Adler-Bell, *The Disparate Impact of Surveillance*, CENTURY FOUND. (Dec. 21, 2017), https://production-tcf.imgix.net/app/uploads/2017/12/03151009/the-disparate-impact-of-surveillance.pdf [https://perma.cc/37LH-JKB8]).

224. JOHANNA MILLER & SIMON MCCORMACK, N.Y. C.L. UNION, SHATTERED: THE CONTINUING, DAMAGING, AND DISPARATE LEGACY OF BROKEN WINDOWS POLICING IN NEW YORK CITY 15 (2018), https://www.nyclu.org/sites/default/files/field_documents/nyclu_20180919_shattered_web.pdf [https://perma.cc/AZF2-X2W4].

225. *Leaders of a Beautiful Struggle*, 2 F.4th at 347; *see also* MILLER & MCCORMACK, *supra* note 224 (detailing how the NYPD employs mass surveillance technologies, especially in heavily policed neighborhoods, which makes "communities feel more like a battlefield than a neighborhood").

226. Assemb. B. A84A, 2021-2022 Leg., Reg. Sess. (N.Y. 2022).

227. Elec. Location Amends., H.B. 251 1st Sub., 2021 Gen. Sess. (Utah 2021), https://le.utah.gov/~2021/bills/hbillamd/HB0251S01.pdf [https://perma.cc/B4SL-4R76].

228. *See supra* section I.B.

CONCLUSION

Keyword warrants demonstrate how law enforcement continuously push the boundaries of privacy. These warrants may be relatively new in the public eye, but they involve the same issues search and seizure law and privacy law have been tackling for centuries. Because keyword warrants, by their nature, cannot be sufficiently particularized, they are unconstitutional under the Fourth Amendment. Keyword warrants are general warrants in sheep's clothing, allowing law enforcement to capture the information of thousands of individuals that searched a specific query, or "keyword" related to a crime. While general warrants have been constitutionally outlawed, new technologies encroach on these restrictions. Dragnet policing has evolved to take advantage of more advanced technological tools, and the police's access to this data provides more avenues for state control. The courts and the legislature must also evolve in tandem with the police, or otherwise our Fourth Amendment privacy rights may be sacrificed in the name of law enforcement.

More scholarship and advocacy need to be invested in both analyzing and fighting against the overbroad nature of keyword warrants. While the Fourth Amendment provides great protections for the American populace, it is not the be all, end all for privacy protections. State constitutions have more robust search and seizure clauses.[229] Advocates will have a much easier time striking down keyword warrants under state constitutions. As Justice William J. Brennan, Jr. asserted, "[t]he legal revolution which has brought federal law to the fore must not be allowed to inhibit the independent protective force of state law—for without it, the full realization of our liberties cannot be guaranteed."[230]

229. Gorman, *supra* note 217, at 464; *see* Davis & Banks, *supra* note 217, at 14.

230. Brennan, Jr., *supra* note 217, at 491.