"IF I DIE, DELETE MY BROWSER HISTORY": THE FOURTH AMENDMENT IMPLICATIONS OF REVERSE KEYWORD SEARCH WARRANTS

ASTRID LONG-KELLOUGH*

I. INTRODUCTION

Information technology and the Internet play a critical role in nearly all aspects of a person's life.[1] Professional activities, commercial transactions, education and scholarship, political support, and advocacy increasingly take place in virtual locales.[2] Medical and mental health care is provided via telehealth systems.[3] Family interactions, friendships, dating, and courtships often occur on dating apps and social media.[4] Online activities

* Astrid Long-Kellough is a third-year, J.D. student at Capital University Law School. She is an Articles Editor for the Capital University Law Review and the Secretary of the Capital Law ACLU Chapter. In May of 2021, she graduated cum laude from The Ohio State University, receiving a Bachelor of Arts in Anthropology. She would like to thank her parents, fiancé, friends, colleagues, and faculty advisor for their support and advice throughout this process.

[1] *See generally* Zaryn Dentzel, *How the Internet Has Changed Everyday Life*, 19 KEY ESSAYS ON HOW THE INTERNET IS CHANGING OUR LIVES 9 (2014), https://www.bbvaopenmind.com/wp-content/uploads/2014/03/BBVA-OpenMind-How-the-Internet-Has-Changed-Everyday-Life-Zaryn-Dentzel.pdf.pdf [https://perma.cc/ML3H-S6W8].

[2] *See generally id.*

[3] *See generally* Hua Li et al., *Transition of Mental Health Service Delivery to Telepsychiatry in Response to COVID-19: A Literature Review*, 93 PSYCH. Q. 181, 182 (June 8, 2021), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8185490/pdf/11126_2021_Article_9926.pdf [https://perma.cc/KE4J-K62Q].

[4] *See* Ilene Manacher, *More Than Half of Teens Make New Friends Online*, CBS NEWS (Aug. 6, 2015, 2:50 PM), https://www.cbsnews.com/news/more-than-half-of-teens-make-new-friends-online-pew-poll/ [https://perma.cc/TX7W-N295]. *See* Donna Ferguson, *How Online Dating Has Changed the Way We Fall in Love*, THE GUARDIAN (Feb. 13, 2022, 7:00 AM), https://www.theguardian.com/lifeandstyle/2022/feb/13/how-online-dating-has-changed-the-way-we-fall-in-love [https://perma.cc/WY8R-DFZG].

are, for almost everyone, a substantial, meaningful, and personal part of their interaction with the world.[5]

As increasingly more of our lives move online, law enforcement has sought—and vendors have compliantly provided—many tools for surveilling and investigating people in the digital realm.[6] In recent years, law enforcement has probed vast troves of DNA data on genealogy websites to identify distant relatives of cold case victims and suspects.[7] Police have used artificial intelligence to attempt to predict who will commit a crime.[8] Facial identification algorithms have been applied to security videos, news photos, and social media posts and used to identify, arrest, and prosecute people attending protests or social gatherings.[9] Texts and social media posts have been subpoenaed and used for investigating and prosecuting individuals.[10]

One need not think hard to imagine the horrific effects of unrestricted state intrusion in private citizens' lives using new technologies. With states passing abortion restrictions and bans in the wake of *Dobbs v. Jackson Women's Health Organization*,[11] it is not difficult to envision a pregnant

---

[5] *See generally* Dentzel, *supra* note 1.

[6] Danielle Abril, *Drones, Robots, License Plate Readers: Police Grapple with Community Concerns as They Turn to Tech for Their Jobs*, THE WASHINGTON POST (Mar. 9, 2022, 7:00 AM), https://www.washingtonpost.com/technology/2022/03/09/police-technologies-future-of-work-drones-ai-robots/ [https://perma.cc/446H-WQNL].

[7] Raffi Khatchadourian, *How Your Family Tree Could Catch a Killer*, THE NEW YORKER (Nov. 15, 2021), https://www.newyorker.com/magazine/2021/11/22/how-your-family-tree-could-catch-a-killer [https://perma.cc/8UB6-DDF2].

[8] Pranshu Verma, *The Never-Ending Quest to Predict Crime Using AI*, THE WASHINGTON POST (July 15, 2022, 7:00 AM), https://www.washingtonpost.com/technology/2022/07/15/predictive-policing-algorithms-fail/ [https://perma.cc/DUN2-9Q72].

[9] *See generally* Nicol Turner Lee & Caitlin Chin, *Police Surveillance and Facial Recognition: Why Data Privacy is Imperative for Communities of Color*, BROOKINGS (Apr. 12, 2022), https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/ [https://perma.cc/N5J9-W2CR].

[10] *See, e.g.*, Michael Kunzelman, *Capitol Rioters' Social Media Posts Influencing Sentencings*, AP NEWS (Dec. 11, 2021), https://apnews.com/article/media-prisons-social-media-capitol-siege-sentencing-0a60a821ce19635b70681faf86e6526e [https://perma.cc/L5QD-N3TZ].

[11] 142 S. Ct. 2228 (2022).

person's online activities being searched to obtain evidence that they were accessing abortion information, abortion drugs, or travel to a state that offers legal abortions.[12] Attempts by many states to restrict the access of trans youth to gender-affirming care often criminalize people who provide counseling or information about such care.[13] Police could use a trans youth's search history to find and punish people providing them with information about gender-affirming care.[14]

Recently, a concerning new breed of warrant–known as a "reverse warrant"– has come into use that raises many of these concerns.[15] While traditional search warrants specify a suspect or location, these warrants cast a wide net to identify all possible suspects.[16]

While the aforementioned genealogy database searches are a form of reverse search, the two best examples of reverse warrants are geofence

---

[12] Jon Schuppe, *Police Sweep Google Searches to Sind Suspects. The Tactic Is Facing Its First Legal Challenge*, NBC (June 30, 2022, 2:27 PM), https://www.nbcnews.com/news/us-news/police-google-reverse-keyword-searches-rcna35749 [https://perma.cc/WL4Y-NFJ5]; *see also* Russell Brandom et al., *The Biggest Privacy Risks in Post-*Roe *America*, THE VERGE (June 27, 2022, 3:47 PM), https://www.theverge.com/23185081/abortion-data-privacy-roe-v-wade-dobbs-surveillance-period-tracking [https://perma.cc/4L3J-GTDA] (discussing how law enforcement could use digital data to identify those who are pursuing an abortion).

[13] Hannah Schoenbaum, *Republican States Aim to Restrict Transgender Health Care in First Bills of 2023*, PBS NEWSHOUR (Jan. 7, 2023, 2:36 PM), https://www.pbs.org/newshour/politics/republican-states-aim-to-restrict-transgender-health-care-in-first-bills-of-2023 [https://perma.cc/F3RS-Q3XJ].

[14] Jennifer Lynch & Andrew Crocker, *UPDATE: Colorado Supreme Court Grants Review in First U.S. Case Challenging Dragnet Keyword Warrant*, EFF DEEPLINKS BLOG, https://www.eff.org/deeplinks/2022/06/eff-file-amicus-brief-first-us-case-challenging-dragnet-keyword-warrant [https://perma.cc/NXM3-7KMH] (Jan. 18, 2023).

[15] Matthew Guariglia, *Geofence Warrants and Reverse Keyword Warrants Are So Invasive, Even Big Tech Wants to Ban Them*, EFF DEEPLINKS BLOG (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/N3XD-Q9JX].

[16] *See* 2023–2024 Legislative Memorandum, N.Y. C.L. Union, Prohibits the Use of Reverse Location and Reverse Keyword Searches – A.3306 (Solages) / S.217 (Myrie) 1 (2023), https://www.nyclu.org/sites/default/files/field_documents/230515-legislativememo-reverse_warrants.pdf [https://perma.cc/9842-WBUF].

(also known as reverse location warrants) and reverse keyword warrants.[17] Geofence warrants seek information on any individual whose cell phone was in a specific geographic area during a particular period.[18] Reverse keyword warrants allow law enforcement to obtain information from search engines about anyone who searched for a term or set of terms specified in the warrant.[19]

In contrast to the typical warrant, these tools reverse the normal assumptions: rather than searching the place or property of a person linked by probable cause to a particular crime, these warrants use broad parameters to identify any person who might have had a potential connection with the evidence.[20]

These new investigative tools have broad ramifications for privacy and Fourth Amendment protections.[21] Vastly more of modern life takes place online than ever took place through the mail or on the telephone.[22] Nevertheless, while mail, telephone, and wire communications are protected with established privacy safeguards, courts have—for the most part—been slow to react to law enforcement efforts that intrude on our virtual world.[23]

Currently, the preeminent case concerning Fourth Amendment violations in the digital age is *Carpenter v. United States*,[24] in which the Supreme Court held the third-party doctrine could not be applied to

---

[17] Albert Fox Cahn & Amanda Humell, *'Keyword Warrants' Make Every Search A Risk*, VERFASSUNGSBLOG (Oct. 15, 2020), https://verfassungsblog.de/keyword-warrants/ [https://perma.cc/6HEU-3UAE].

[18] *Id.*

[19] *Id.*

[20] Johana Bhuiyan, *The New Warrant: How US Police Mine Google for Your Location and Search History*, THE GUARDIAN (Sept. 16, 2021, 6:00 AM), https://www.theguardian.com/us-news/2021/sep/16/geofence-warrants-reverse-search-warrants-police-google [https://perma.cc/GA78-BURU].

[21] Guariglia, *supra* note 15.

[22] *See* Summer Allen, *Social Media's Growing Impact on Our Lives,* AM. PSYCH. ASS'N (Sept. 20, 2019), https://www.apa.org/members/content/social-media-research [https://perma.cc/WHG3-LTFQ].

[23] Tal Kopan, *Digital Era Confounds the Courts*, POLITICO (Nov. 30, 2013, 3:59 PM), https://www.politico.com/story/2013/11/digital-era-technology-supreme-court-cases-100410 [https://perma.cc/Z6BM-DP8C].

[24] 138 S. Ct. 2206 (2018).

historic cell tower location data because of the "near-perfect" detail of the information obtained.[25] In his majority opinion, Chief Justice Roberts acknowledged the role that cell phones play in the modern world, likening them to "a 'feature of human anatomy.'"[26] For the first time, the Court acknowledged that people using the Internet or a device can have an expectation of privacy under the Fourth Amendment even though the data is held by another entity.[27] While exploration of *Carpenter's* potential implications for the Fourth Amendment and privacy in the digital age has only just begun, this case does not neatly resolve the legality of reverse keyword warrants.[28]

In this note, I will argue keyword warrants, used increasingly in police investigations with little oversight, can violate the Fourth Amendment. They strike nakedly at the very foundation of rights guaranteed by The Framers. Unlike some constitutional rights, which require probing explorations of history and linguistics to understand The Framers' intent, the intent regarding reverse warrants is quite clear. The Fourth Amendment was drafted in response to the use of general warrants by the British in the 1700s.[29] These warrants allowed agents of the crown to search any place, whenever they wished, for any reason or for none at all.[30] Like general

---

[25] Louise Matsakis, *The Supreme Court Just Greatly Strengthened Digital Privacy*, WIRED (June 22, 2018, 12:26 PM), https://www.wired.com/story/carpenter-v-united-states-supreme-court-digital-privacy/ [https://perma.cc/3XBP-P72S]; Carpenter v. United States, 138 S. Ct. 2206, 2217–18 (2018).

[26] *Carpenter*, 138 S. Ct. at 2218 (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

[27] Matsakis, *supra* note 25.

[28] Jenifer Lynch, *Courts Grapple with a Sea Change in Fourth Amendment Law After* Carpenter v US*: Year in Review 2019*, EFF DEEPLINKS BLOG (Dec. 29, 2019), https://www.eff.org/deeplinks/2019/12/courts-grapple-sea-change-fourth-amendment-law-after-carpenter-v-us-year-review [https://perma.cc/SDD2-V3SC].

[29] Payton v. New York, 445 U.S. 573, 583 (1980) ("It is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment.").

[30] *See* Brian Frazelle & David Gray, *What the Founders Would Say About Cellphone Surveillance*, ACLU (Nov. 17, 2017), https://www.aclu.org/news/privacy-technology/what-founders-would-say-about-cellphone-surveillance [https://perma.cc/NGW8-YA5U].

warrants, reverse keyword warrants lack any particularized probable cause and implicate the privacy of possibly billions of innocent people.[31]

Unless curbed by the courts or legislature, we can only expect the use of reverse warrants—including reverse keyword warrants—to become more widespread as word spreads among police departments about their potential for obtaining private information of potential relevance.[32] A rich body of jurisprudence dating back over a century protects Americans' Fourth Amendment rights to security in their postal and telephone communications.[33] No such body of law exists for the digital world.[34] Reverse keyword warrants recently faced their first constitutional challenge in the Colorado Supreme Court case of *People of The State of Colorado v. Seymour* and were the subject of two bills proposed during the 2023 sessions of the New York and California State Legislatures.[35] Until

---

[31] Motion to Suppress Evidence from a Keyword Warrant & Request for a Veracity Hearing ¶ 67, People v. Seymour, 2023 CO 53 (No. 21CR20001), [hereinafter Motion to Suppress], https://s3.documentcloud.org/documents/22076537/motion-to-suppress-google-evidence-in-colorado-vs-seymour.pdf [https://perma.cc/94RW-CAMF].

[32] *See* Brief of Amicus Curiae Electronic Frontier Foundation in Support of Defendant's Motion to Suppress at 8–9, People v. Seymour, 2023 CO 53 (No. 21CR20001), [hereinafter Amicus Brief Supporting Defendant], https://www.eff.org/files/2022/06/30/21cr20001_seymour_eff_amicus_brief.pdf [https://perma.cc/FVW5-HB5T].

[33] *See* Andrew Crocker & Hanni Fakhoury, *Government Explains Away Fourth Amendment Protection for Digital Communications*, EFF DEEPLINKS BLOG (May 13, 2014), https://www.eff.org/deeplinks/2014/05/government-explains-away-fourth-amendment-protection-digital-communications [https://perma.cc/X5WX-J7WA].

[34] *See* Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 NYU ANN. SURV. AM. L. 553, 554 (2017), https://annualsurveyofamericanlaw.org/wp-content/uploads/2017/04/71-4_donohue.pdf [https://perma.cc/4WKB-EDDB] ("Fourth Amendment doctrine no longer reflects how the world works. Technology has propelled us into a new era.").

[35] People v. Seymour, 536 P.3d 1260 (Colo, 2023); Corin Faife, *Powerful Keyword Warrants Face New Challenge in Deadly Arson Case*, THE VERGE, https://www.theverge.com/2022/7/1/23191406/denver-arson-google-keyword-warrant-challenge-constitutional-fourth-amendment-privacy [https://perma.cc/4FWM-DS2W] (July 1, 2022, 4:15 PM).

Much of the research and drafting for this Note took place after the Denver District Court denied Seymour's motion to suppress the keyword evidence in November of 2022. (*continued*)

the Supreme Court or legislators resolve this issue, however, reverse keyword warrants will remain in a sort of legal limbo.[36] Given the slow pace with which the Court has addressed emergent technologies, legislation like that proposed in New York and California presents the most immediate solution for curtailing the use of these dangerous and unconstitutional warrants.[37]

Julia Cardi, *Denver Judge Upholds Search Warrants Used in Green Valley Ranch Arson Investigation*, DENVER GAZETTE (Nov. 16, 2022), https://denvergazette.com/premium/denver-judge-upholds-search-warrants-used-in-green-valley-ranch-arson-investigation/article_c6ab83a6-65ff-11ed-baff-6702f5b0cf78.html [https://perma.cc/C5NU-Z3AV]. In January of 2023, Seymour petitioned for and was granted certiorari to the Colorado Supreme Court. Kyla Pearce, *Reverse-Keyword Search Warrant Used to Identify Suspects in Deadly Arson Case Goes to Colorado Supreme Court*, DENVER GAZETTE (May 4, 2023), https://www.denverpost.com/2023/01/20/denver-police-reverse-keyword-search-colorado-supreme-court/ [https://perma.cc/H3V8-RV6N]. After this Note was accepted for publication, oral arguments took place before the Colorado Supreme Court. *Colorado Supreme Court to Hear Arguments at Colorado Mesa University on May 4*, COLO. JUD. BRANCH (May 1, 2023), https://www.courts.state.co.us/Media/release.cfm?id=2040 [https://perma.cc/UF2M-AWYG]. In October 2023, as this Note was undergoing its final edits, the court released its opinion upholding the admission of the keyword evidence under the good faith exception to the Fourth Amendment exclusionary rule. *See* Seymour, 536 P.3d at 1267.

Subsequently, in early 2024, the Pennsylvania Supreme Court announced it would hear a case challenging the constitutionality of reverse keyword warrants. John Beauge, *Constitutionality of Police Using Keyword Warrants Challenged in Pa. Case*, PENNLIVE (Jan. 7, 2024, 6:27 PM), https://www.pennlive.com/news/2024/01/constitutionality-of-police-using-keyword-warrants-challenged-in-pa-case.html [https://perma.cc/58ZS-M2Y7]. The appellant, John Kurz was identified as a suspect in a rape and kidnapping in 2016 when law enforcement obtained a warrant seeking the IP addresses of anyone who searched the victim's name or address in the week before the attack. *Id.* The Electronic Frontier Foundation and the National Association of Criminal Defense Lawyers—two groups heavily involved in the *Seymour* case have submitted amicus briefs urging the Pennsylvania Supreme Court to find the practice unconstitutional. *Id.*

[36] Guariglia, *supra* note 15.

[37] Sam Baker & Ashley Gold, *Big Tech's Future Is up to a Supreme Court that Doesn't Understand It*, AXIOS, https://www.axios.com/2023/02/20/supreme-court-section

(*continued*)

This note proceeds in two parts. Part I presents a technical discussion of how an Internet query works and Google's process for responding to a reverse keyword warrant. Next, it discusses the similarities between reverse keyword warrants and the analogous field of geofence warrants. This section also considers the potential for abuse of reverse keyword warrants with a particular focus on their implications in a post-*Roe v. Wade* world. Finally, it details known uses of reverse keyword warrants and describes their current legal status.

Part II analyzes the constitutionality of reverse keyword warrants under the Fourth Amendment. First, it uses the Supreme Court's holding in *Carpenter v. United States* to posit that people have a reasonable expectation of privacy in their search histories and that the third-party doctrine does not apply. Thus, it contends a search of users' internet histories typically requires a valid warrant. Next, this section argues reverse keyword warrants do not meet the technical requirements for a search warrant. It first details the historical events which gave rise to the Fourth Amendment and examines reverse keyword warrants as a form of modern-day general warrant. Finally, this paper discusses how reverse keyword warrants lack particularized probable cause and fail to describe with particularity the "place to be searched, and the persons or things to be seized."[38]

II. BACKGROUND ON SEARCH ENGINES, REVERSE WARRANTS, AND INCURSIONS ON PRIVACY BY REVERSE KEYWORD WARRANTS

This section provides an overview of how search engines like Google or Bing function and the staged process Google uses in response to reverse keyword warrants served on it by law enforcement. It additionally discusses the functional similarities between reverse keyword warrants and geofence warrants. It then describes known uses of reverse keyword

---

-230-google-twitter-tech [https://perma.cc/AQS8-UWQ4] (Feb. 21, 2023) ("The Supreme Court is an inherently slow-moving institution that tries to solve problems mainly by searching for one broad principle that can last forever. And that's simply hard to square with complex, evolving technology."); 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, 1412–13 (2023) (discussing the expediency of a legislative solution).

[38] U.S. CONST. amend. IV.

warrants and their broader potential for abuse. The section concludes by outlining the current legal status of reverse warrants and reverse keyword warrants.

A. The Technology Behind Internet Queries and Reverse Keyword Warrants

To fully analyze the legal ramifications of reverse keyword warrants, it is important to understand the basics of how a search engine fields a user's query and uses the information it collects in this process when responding to reverse keyword warrants.[39] Although Bing and Yahoo also have mechanisms for responding to reverse keyword warrants, this note will focus on Google because it makes up about 93% of the global search engine market.[40] Finally, this section provides background information on geofence warrants, another type of reverse warrant with a more developed body of caselaw that will be used as an analogy throughout this note.

1. Search Engines & Queries

At a fundamental level, a search engine is an index of webpages on the Internet.[41] In order to provide more detailed results, search engines use pieces of software called "crawlers" to discover new websites and add them to their databases.[42] When a user makes a query, the search engine uses the keywords entered to pull up relevant websites from its database.[43] These results are then ranked by the search engine's algorithm using a variety of factors.[44] To serve ads and personalize search results, a user's history of queries is associated with their account or, if the user is not

---

[39] Amicus Brief Supporting Defendant, *supra* note 32, at 7–8.

[40] Ron Amadeo, *ChatGPT-style Search Represents a 10x Cost Increase for Google, Microsoft*, ARS TECHNICA (Feb. 22, 2023, 3:09 PM), https://arstechnica.com/gadgets/2023/02/chatgpt-style-search-represents-a-10x-cost-increase-for-google-microsoft/ [https://perma.cc/44MQ-NC3E].

[41] *In-depth Guide to How Google Search Works*, GOOGLE SEARCH CENT. https://developers.google.com/search/docs/fundamentals/how-search-works [https://perma.cc/JR7L-XR7V].

[42] *Id.*

[43] Matt Cutts, *How Search Works*, YOUTUBE, at 00:49 (June 5, 2013), https://www.youtube.com/watch?v=mFGUeVdSQJw [https://perma.cc/FZ9H-F2BM].

[44] *Id.* at 00:59.

logged in, their IP address.[45] This collection occurs by default.[46] While Google allows users to delete their history and disable collection, this only prevents the data from being associated with a user's account: their IP address, which can be used to identify the person, is still tracked.[47]

In Google's Terms of Service, it states that "[y]our content remains yours, which means that you retain any intellectual property rights that you have in your content."[48] Thus, throughout this note, this keyword data will be referred to as the "users' data."

2. Reverse Keyword Warrants

Until 2022, little was known about Google's process for responding to reverse keyword warrants and what information law enforcement could obtain.[49] In a declaration submitted by Nikki Adeli, a Policy Specialist on Google's Legal Investigation Support Team, as part of the *People v. Seymour* case, she revealed how the company responds to reverse keyword warrants.[50] In *Seymour* (discussed further *infra*), a Colorado teenager was charged with murder after he was identified through a reverse keyword warrant seeking information pertaining to anyone who searched for the address where a fatal house fire took place.[51]

Adeli stated Google uses a staged process in responding to warrants.[52] During the first stage, members of the Legal Investigation Support Team

---

[45] *See* Google, *Information Google Collects Google Privacy Policy*, YOUTUBE (Mar. 5, 2020) https://www.youtube.com/watch?v=Qa74-VRbg7A [https://perma.cc/2838-L346]; Declaration of Legal Investigations Support Analyst ¶ 7, People v. Seymour, 2023 CO 53 (No. 21CR20001), https://www.eff.org/files/2022/07/06/2022-07-05_13-22-16_attachment_-_declaration_of_nikki_adeli19.pdf [https://perma.cc/H7MT-2A6X].

[46] Amicus Brief Supporting Defendant, *supra* note 32, at 7–8.

[47] *Id.*

[48] *Google Terms of Service*, GOOGLE PRIV. & TERMS (Jan. 5, 2022), https://www.gstatic.com/policies/terms/pdf/20220105/it7r24p9/google_terms_of_service_en_us.pdf [https://perma.cc/S27T-Q9MP].

[49] *See* Motion to Suppress, *supra* note 31, ¶ 15.

[50] *Id.*

[51] Darren Whitehead, *Green Valley Ranch Murder Case: Google Evidence Will Be Allowed at Teen's Trial*, 9NEWS, https://www.9news.com/article/news/crime/green-valley-ranch-arson-murder/73-b3e6f847-d510-4a2b-bec6-e9351352ffd5 [https://perma.cc/Q654-SYP2] (Nov. 16, 2022, 6:07 PM).

[52] Declaration of Legal Investigations Support Analyst, *supra* note 45, ¶ 3.

create "a text-based query (that can include letters, numbers, or characters) based on the requirements of the warrant."[53] In order to compile this document, Google must query "its entire database of users' search queries within the relevant time period …including users well outside the area of the crime."[54]

In the next stage, Google compiles a comma-separated values (CSV) text file based on the query.[55] Based on the terms of the warrant, the search engine "may limit the results to queries that contain only the search terms listed in the warrant" or the results "may extend to queries that include the specified search terms as part of a query that contains other words."[56] For example, if authorities requested results for anyone who searched "123 Main Street," and the query returned searches for "123 Main Street Anytown, U.S.A," both results could be included in the data turned over to law enforcement if the warrant specified such.[57] This data would be turned over to law enforcement whether it was relevant to the investigation or not.[58]

Finally, Google stated it de-identifies the query data and provides the CSV file to law enforcement.[59] This production document

> typically includes the following categories of information: (1) the date and time of the [keyword] search, (2) coarse location information inferred from the IP address from which the search was conducted, (3) the Query..., (4) the Result..., (5) the Host..., (6) the Request..., (7) a truncated Google identifier (known as the GAIA ID), if the search was conducted from an authenticated user's account, or a truncated version of a Browser Cookie ID if the search

---

[53] *Id.* ¶ 4.

[54] Amicus Brief Supporting Defendant, *supra* note 32, at 10.

[55] Declaration of Legal Investigations Support Analyst, *supra* note 45, ¶ 6. A CSV or Comma Separated Value file is a plain text list of data like a spreadsheet. Dave Johnson, *What Is a CSV File? How to Open and Use the Popular Spreadsheet File*, BUS. INSIDER (Apr. 8, 2022, 11:14 AM), https://www.businessinsider.com/guides/tech/what-is-csv-file [https://perma.cc/7MBJ-BETT].

[56] Declaration of Legal Investigations Support Analyst, *supra* note 45, ¶ 6.

[57] *Id.*

[58] Motion to Suppress, *supra* note 31, ¶ 17.

[59] Declaration of Legal Investigations Support Analyst, *supra* note 45, ¶ 8.

> was not conducted from an authenticated user's account and (8) the associated user agent string.[60]

Although the initial data is de-identified, law enforcement can compel Google to provide identifying information like IP addresses on users it believes are relevant in several ways.[61] If authorized by the initial warrant, law enforcement need n.ot seek further court authorization and can simply request the identifying information.[62] For users logged into their account at the time they made the search, Google provides "the IP address associated with the search (if available), the full GAIA ID [a unique identifier Google uses for account holders], and basic subscriber information for that GAIA ID." [63] For users who were not logged in at the time they made the search Google provides the user's IP address and "a full Browser Cookie ID."[64] If not authorized by the initial warrant, authorities can still obtain identifying information by getting a second warrant or subpoenaing the information under 18 U.S.C. § 2703(c)(2).[65]

Google purports to safeguard users' privacy by requiring law enforcement to obtain additional authorization at each stage.[66] However, Google admittedly does not always use this staged procedure.[67] For example, in the *Seymour* case, Google complied with a reverse keyword warrant demanding the search engine turn over IP addresses in the first stage, rendering the staged process irrelevant.[68]

3. Geofence Warrants are Analogous to Reverse Keyword Warrants

When confronted with new surveillance technology, courts frequently rely on analogies to earlier cases in their Fourth Amendment analysis.[69]

---

[60] Motion to Suppress, *supra* note 31, ¶ 18 (quoting Declaration of Legal Investigations Support Analyst, *supra* note 45, ¶ 7).

[61] *Id.* ¶ 19.

[62] *Id.*

[63] Declaration of Legal Investigations Support Analyst, *supra* note 45, ¶ 9.

[64] *Id.*

[65] Motion to Suppress, *supra* note 31, ¶ 19.

[66] Declaration of Legal Investigations Support Analyst, *supra* note 45, ¶ 3.

[67] *Id.* (stating that "Google generally employs a staged process . . . .").

[68] Motion to Suppress, *supra* note 31, ¶ 16.

[69] *See, e.g.*, Jeffrey Vagle, *The Difficulty with Metaphors and the Fourth Amendment*, JUST SEC. (Aug. 31, 2015), https://www.justsecurity.org/

(*continued*)

While reverse keyword warrants are currently being challenged for the first time, the law surrounding another type of reverse warrant is more developed.[70] Geofence warrants have been found unconstitutional in federal and state courts and operate in largely the same way as reverse keyword warrants, making them a helpful analog.[71]

At the most basic level, geofence warrants and keyword warrants are reverse warrants.[72] When using a traditional warrant, authorities identify a specific suspect or place to be searched; however, when using a reverse warrant, law enforcement instead sets a broad parameter from which they identify possible suspects.[73] In the case of geofence warrants, law enforcement requests information for all the devices located within a geographic area (the geofence) for a specified period.[74] This information is derived from a user's location history.[75] Whereas, with reverse keyword warrants, authorities provide the search engine a list of keywords and request information on any users who searched for the keywords or a variation thereof within a particular period.[76] This information is derived from the user's search history.[77]

25718/fourth-amendment-difficulty-
metaphors/ [https://perma.cc/5GFW-FJ8Y] ("Everyone—including judges—is drawn to the use of metaphors and analogies when it comes to applying Fourth Amendment doctrine to the less-than-tangible.").

[70] *See Reverse Search Warrants*, NAT'L ASS'N CRIM. DEF. LAWS. (Nov. 2, 2022), https://www.nacdl.org/Content/Reverse-Search-Warrants-
NY [https://perma.cc/EGJ9-AVNW]; Isha Marathe, *Despite Rulings, 4th Amendment Battles Over GeoFence Warrants Are Far from Over*, L. TECH. NEWS (May 26, 2022, 4:45 PM), https://www.law.com/legaltechnews/2022/05/26/
despite-rulings-fourth-amendment-battles-over-geofence-warrants-are-far-from-over/ [https://perma.cc/5LGV-XV6K].

[71] *Id.*

[72] Bhuiyan, *supra* note 20.

[73] *See* Motion to Suppress, *supra* note 31, ¶ 6.

[74] *Id.* ¶ 11.

[75] *Id.*

[76] *Id.* ¶ 1.

[77] *See id.* ¶ 4.

Google claims that it uses a similar three-stage process for responding to both types of warrants.[78] In both, a data specialist first presents law enforcement with a de-identified list of users it deems responsive to the warrant.[79] In the second stage, law enforcement is allowed to review the list and narrow it if they wish.[80] In the final stage, they can request identifying data for all or some of the users.[81]

Privacy advocates raise similar concerns regarding the constitutionality of keyword and geofence warrants, suggesting they are overly broad and lack sufficient probable cause.[82] Additionally, both have similar potential to chill expressive freedoms and be used against people seeking an abortion or gender-affirming care in a jurisdiction where such care is criminalized.[83]

B. The Use and Potential Abuse of Reverse Keyword Warrants

This section begins by discussing cases in which reverse keyword warrants were used. It then delves into the broader privacy implications of reverse keyword warrants with a particular eye toward how these warrants could be abused in a post-*Roe v. Wade* world.

1. Known Uses of Reverse Keyword Warrants

One of the earliest reported uses of a reverse keyword warrant occurred in 2017, in the town of Edina, Minnesota.[84] Following a fraud

---

[78] *Compare* Declaration of Legal Investigations Support Analyst, *supra* note 45, ¶ 3 (stating that "Google generally employs a staged process . . . .") *with* United States v. Chatrie, 590 F. Supp. 3d 901, 914 (E.D. Va. 2022).

[79] Declaration of Legal Investigations Support Analyst, *supra* note 45, ¶ 7; *Chatrie*, 590 F. Supp. 3d. at 914–15.

[80] Declaration of Legal Investigations Support Analyst, *supra* note 45, ¶ 8; *Chatrie*, 590 F. Supp. 3d at 916.

[81] Declaration of Legal Investigations Support Analyst, *supra* note 45, ¶ 9; *Chatrie*, 590 F. Supp. 3d at 916.

[82] Guariglia, *supra* note 15.

[83] *Id.*; Hayley Tsukayama, *EFF Backs California Bill to Protect People Seeking Abortion and Gender-Affirming Care from Dragnet Digital Surveillance*, EFF DEEPLINKS BLOG (Feb. 13, 2023), https://www.eff.org/deeplinks/2023/02/eff-backs-california-bill-protect-people-seeking-abortion-and-gender-affirming [https://perma.cc/G587-Z3TX].

[84] Thomas Brewster, *Cops Demand Google Data on Anyone Who Searched a Person's Name... Across a Whole City*, FORBES (Mar. 17, 2017, 7:15 AM), https://www.forbes.com/

(*continued*)

attempt at a local credit union, the Edina Police Department obtained a warrant for the names, email addresses, social security numbers, payment information, account data, and IP addresses of everyone in the town who had searched a variation of the victim's name within a one-month period.[85] Although Google publicly stated it would resist the Edina Police Department's request, it ultimately complied after the scope of the warrant was narrowed.[86] It is unclear whether a suspect was ever identified or apprehended in this case.[87]

Another known use of reverse keyword warrants took place in Austin, Texas, in 2018.[88] Federal Agents investigating a series of bombings sought information from Google, Microsoft, and Yahoo about users in Texas who searched terms including "explosive," "bomb," "pipe bomb," and variations thereof.[89] The agents ultimately identified the serial bomber when authorities obtained surveillance footage of a man mailing a package that later blew up in a FedEx facility; the suspect committed suicide before he could be apprehended.[90] The information Google provided in response to the reverse keyword warrant remains under seal, so it is not known how

---

sites/thomasbrewster/2017/03/17/google-government-data-grab-in-edina-fraud-investigation/?sh=7030701b7ade [https://perma.cc/3EWK-ZJZ6].

[85] *Id.*

[86] Miguel Otárola, *Police Get Search Warrant for Everyone Who Googled Edina Resident's Name*, STAR TRIBUNE (Mar. 18, 2017, 8:02 AM), https://www.startribune.com/search-warrant-issued-to-edina-police-raises-privacy-concerns-of-internet-users/416442113/ [https://perma.cc/C4JK-FHKS]; Miguel Otárola, *After Edina Police Demand Search Data, Google Turns over One Record*, STAR TRIBUNE (May 12, 2017, 8:38 PM), https://www.startribune.com/google-narrows-edina-search-warrant-to-only-obtain-one-record/422111323/ [https://perma.cc/G6P6-Y62R].

[87] Despite an extensive search of local and national news as well as public records during the research process for this Note, no additional information could be found about a suspect's identification or apprehension.

[88] Brewster, *supra* note 84.

[89] *Id.*; Affidavit in Support of an Application for a Search Warrant ¶ 2, *In re* The Search Of Info. & Recs. Assoc'd. With Google Searches For Various Search Terms That Are Stored At Premises Controlled By Google, No. 1:18-mj-00191-ML (W.D. Tex. filed Mar. 19, 2018), https://www.justice.gov/file/1124151/download [https://perma.cc/X77E-EZSR].

[90] David Leffler, *20 Days in Hell: Looking Back at Austin's Serial Bombings*, AUSTIN MONTHLY (July 2021), https://www.austinmonthly.com/20-days-of-hell-looking-back-at-austins-serial-bombings/ [https://perma.cc/3KDQ-ECRT].

many people were implicated in the search or whether the suspect was one of them.[91]

Documents accidentally unsealed by the Justice Department revealed that in 2019 federal agents in Wisconsin used a reverse keyword warrant to obtain account information and IP addresses for users who had searched a sexual abuse victim's name, "two spellings of her mother's name, or her address over 16 days across the year."[92] Google responded to the warrant in 2020, but the documents did not show how many users' information the search engine turned over.[93] The documents were resealed once the Justice Department's mistake came to light and the investigation remains ongoing.[94]

One paragraph in a different unsealed court filing showed that in 2020, agents used a similar reverse keyword warrant while investigating an associate of R. Kelly for setting fire to the car of a witness in Kelly's racketeering and sexual abuse case.[95] Google responded with a list of IP addresses for people who searched for the victim's address close to the time the arson took place, including an IP address belonging to the associate, Michael Williams.[96] Williams ultimately pleaded guilty to witness tampering rather than going to trial.[97]

---

[91] Brewster, *supra* note 84.

[92] Thomas Brewster, *Exclusive: Government Secretly Orders Google to Identify Anyone Who Searched a Sexual Assault Victim's Name, Address, or Telephone Number*, FORBES (Oct. 4, 2021, 10:33 AM), https://www.forbes.com/sites/thomasbrewster/2021/10/04/google-keyword-warrants-give-us-government-data-on-search-users/?sh=2ff78dca7c97 [https://perma.cc/4YN8-MH4N].

[93] *Id.*

[94] *Id.*

[95] Alfred Ng, *Google Is Giving Data to Police Based on Search Keywords, Court Docs Show*, CNET (Oct. 8, 2020, 1:21 PM), https://www.cnet.com/news/privacy/google-is-giving-data-to-police-based-on-search-keywords-court-docs-show/ [https://perma.cc/WH2S-S742].

[96] Affidavit in Support of an Application for a Search Warrant ¶ 17, *In re* The Search Of Info. Assoc'd With The Cell. Device Assig'd Call No. (229) 418-8231, That Is Stored At Premises Controlled By T-Mobile, No. 20-MC-1584 (S.D.N.Y. filed July 13, 2020).

[97] Nina Pullano, *R. Kelly Friend Accused of Witness Intimidation Pleads Guilty to Arson*, COURTHOUSE NEWS SERVICE (Apr. 19, 2021), https://www.courthousenews.com/r-kelly-friend-accused-of-witness-intimidation-pleads-guilty-to-arson/ [https://perma.cc/9ETU-5EHB].

The common denominator between these cases is that the reverse keyword searches were conducted under seal, thus "insulat[ing] the practice from public debate and regulation."[98] The case records available to the public have largely been revealed through mistake or references in other documents.[99] To this end, Google has not yet revealed the number of reverse keyword warrants it receives.[100] In contrast, the search engine is more forthcoming about the prevalence of geofence warrants.[101]

Geofence warrants are similar to reverse keyword warrants.[102] However, rather than disclosing the information of users who searched a particular keyword, these warrants reveal the IP addresses of people who have been in a location during a specified period.[103] In August of 2021, Google reported it received 11,554 geofence warrants from law enforcement the previous year, an increase from the 8,396 received in 2019.[104] If these figures are indicative of broader trends in the use of reverse warrants, these searches will only become a more pernicious invasion on the privacy around the world.[105]

2. Potential Incursions on Privacy by Reverse Keyword Warrants

In the modern world, virtually any information a person could desire can be found on the Internet.[106] Given the sheer number of webpages, however, it is impossible to meaningfully sift through them without a search engine.[107] Because of the Internet's prominence in all aspects of modern life, Internet queries represent not only research for work or school, but also deeply personal searches relating to the users' physical and mental health, identity, sexuality, religion, and politics.[108] All of these

---

[98] Brewster, *supra* note 92.

[99] *See id.*

[100] Amicus Brief Supporting Defendant, *supra* note 32, at 8.

[101] Bhuiyan, *supra* note 20.

[102] *See Reverse Search Warrants*, NAT'L ASSOC. CRIM. DEF. ATTYS., https://www.nacdl.org/Landing/Reverse-Search-Warrants [https://perma.cc/UL64-6777].

[103] Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2514–15 (2021).

[104] Bhuiyan, *supra* note 20.

[105] Amicus Brief Supporting Defendant, *supra* note 32, at 8–9.

[106] *See generally* Dentzel, *supra* note 1.

[107] Lynch & Crocker, *supra* note 14.

[108] *Id.*

queries are logged in the user's search history and subject to search by law enforcement if they fall within the parameters of a reverse keyword warrant.[109] The consequences of an overly broad and largely unchecked Fourth Amendment search with a vast trove of sensitive information about people's interests, inquiries, and intentions is ripe for abuse.

For instance, the Internet can act as an important resource for transgender youth exploring their identities, or parents, seeking to support their children, as it allows them to access information that may otherwise be unavailable in their communities.[110] However, as of the date of this Note, there are 85 bills in state legislatures around the country seeking to curtail transgender Americans' access to gender-affirming care.[111] The most egregious legislation includes provisions for prosecuting parents, teachers, therapists, or doctors who assist a youth in obtaining care.[112] If some of these bills are successful, law enforcement could use reverse keyword warrants to identify anyone who searched for the names of doctors who provide gender affirming care, addresses of clinics, or terms related to hormone replacement therapy.[113]

Another troubling potential application of these warrants is against protesters. In recent years, authorities have adopted a variety of new technologies to surveil protesters and activists.[114] For example, a report by the U.S. Government Accountability Office revealed that in 2020, six federal law enforcement agencies, including the Federal Bureau of Investigation (FBI), used facial recognition to identify Black Lives Matter

---

[109] *Id.*

[110] *Online Communities and LGBTQ+ Youth*, HUM. RTS. CAMPAIGN, https://www.hrc.org/resources/online-communities-and-lgbtq-youth [https://perma.cc/R7ZA-JC2F].

[111] *Mapping Attacks on LGBTQ Rights in U.S. State Legislatures*, ACLU, https://www.aclu.org/legislative-attacks-on-lgbtq-rights?impact=health [https://perma.cc/GR5A-KFZ6].

[112] Daniel Trotta, *U.S. Republicans Target Transgender Youth Healthcare in Legislative Push*, REUTERS (Feb. 16, 2023, 9:53 AM), https://www.reuters.com/world/us/us-republicans-target-transgender-youth-healthcare-legislative-push-2023-02-16/ [https://perma.cc/K5EG-B9HY].

[113] Lynch & Crocker, *supra* note 14.

[114] Matthew Guariglia, *High Tech Police Surveillance of Protests and Activism: Year in Review 2020*, EFF DEEPLINKS BLOG (Dec. 25, 2020), https://www.eff.org/deeplinks/2020/12/high-tech-police-surveillance-protests-and-activism-year-review-2020 [https://perma.cc/ND29-VLLC].

protesters.[115] Some reverse warrants have already been deployed in this manner.[116] In 2020, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) agents in Kenosha, Wisconsin used twelve geofence warrants to identify racial justice protesters in multiple locations around the city within the two hours of the protest taking place.[117] Similarly, as part of their investigation into the January 6th Insurrection, the FBI served Google with a geofence warrant asking for information on all the devices within four acres of the Capitol between 2:00PM and 6:30PM.[118] Google turned over information on a staggering 5,723 devices.[119] One January 6th defendant moved to suppress the geofence evidence, but his motion was denied.[120] It is not a stretch to imagine authorities using a reverse keyword warrant to identify users who searched for the address of a protest. The use of reverse warrants in this fashion has disturbing implications for mass gatherings, protests, and free assembly in general.

a. Implications of Reverse Keyword Warrants in A Post-Roe World

Law enforcement's increased use of reverse warrants comes at a time when personal liberty has eroded for many Americans.[121] In the wake of the Court's June 2022 decision in *Dobbs v. Jackson Women's Health,* overturning *Roe v. Wade,* trigger laws prohibiting abortion went into effect

---

[115] Radhamely De Leon, *Six Federal Agencies Used Facial Recognition on George Floyd Protestors*, VICE: MOTHERBOARD (June 30, 2021, 9:00 AM), https://www.vice.com/en/article/3aqpmj/six-federal-agencies-used-facial-recognition-on-george-floyd-protestors [https://perma.cc/NM43-SJ8D].

[116] Mark Harris*, A Peek Inside the FBI's Unprecedented January 6 Geofence Dragnet*, WIRED (Nov. 28, 2022, 7:00 AM), https://www.wired.com/story/fbi-google-geofence-warrant-january-6/ [https://perma.cc/WM9L-24VU].

[117] Matthew Guariglia et al., *Geofence Warrants Threaten Civil Liberties and Free Speech Rights in Kenosha and Nationwide*, EFF DEEPLINKS BLOG (Sept. 10, 2021), https://www.eff.org/deeplinks/2021/09/geofence-warrants-threaten-civil-liberties-and-free-speech-rights-kenosha-and [https://perma.cc/L6BM-5G9M].

[118] Harris, *supra* note 116.

[119] *Id.*

[120] Avery Schmitz, *U.S. Federal Judge Denies Motion to Suppress Jan. 6 Location Data*, LAWFARE BLOG (Jan. 25, 2023, 5:05 PM), https://www.lawfareblog.com/us-federal-judge-denies-motion-suppress-jan-6-location-data [https://perma.cc/HH8D-DG8R].

[121] Amicus Brief Supporting Defendant, *supra* note 32, at 8–9.

in 13 states.[122] Other states have enacted or are in the process of enacting tighter restrictions on access to abortion.[123] As a result of these bans and restrictions, many commentators have raised concerns about the potential for criminalization of people who seek abortions and those that assist them.[124] As of the date of this Note, Nevada, and South Carolina have laws criminalizing self-managed abortion (a medication-induced abortion without medical supervision); however, in the absence of laws specifically criminalizing self-managed abortion, other criminal laws such as mishandling of human remains, concealment of a birth, and practicing medicine without a license can be used to criminalize this practice.[125]

This specter of criminalization has brought digital privacy to the fore of many people's minds.[126] Period tracking apps have faced scrutiny over their data-storage policies due to the significant amount of sensitive

---

[122] Nicole Dube et al., *State Abortion Laws Enacted Post*-Dobbs *Decision*, CONN. GEN. ASSEMBLY (Sept. 29, 2022), https://cga.ct.gov/2022/rpt/pdf/2022-R-0227.pdf [https://perma.cc/G5X3-3F6N].

[123] *After* Roe *Fell: Abortion Laws by State*, CTR. FOR REPROD. RTS. https://reproductiverights.org/maps/abortion-laws-by-state/ [https://perma.cc/V78X-NWJ8].

[124] Melissa Jeltsen, *The Coming Rise of Abortion as a Crime*, THE ATLANTIC (July 1, 2022), https://www.theatlantic.com/family/archive/2022/07/roe-illegal-abortions-pregnancy-termination-state-crime/661420/ [https://perma.cc/6QZ8-JW3R].

[125] Ari Shapiro et al., *New Report Tracks Criminal Prosecutions of Self-managed Abortions*, NPR (Aug. 9, 2022, 4:21 PM) https://www.npr.org/2022/08/09/1116590982/new-report-tracks-criminal-prosecutions-of-self-managed-abortions [https://perma.cc/3UAP-CT2M]; LAURA HUSS ET AL., SELF-CARE, CRIMINALIZED: AUGUST 2022 PRELIMINARY FINDINGS 1, 5 (2022), https://www.ifwhenhow.org/wp-content/uploads/2023/06/22_08_SMA-Criminalization-Research-Preliminary-Release-Findings-Brief_FINAL.pdf [https://perma.cc/NE5G-VR72].

[126] Alfred Ng, *'A Uniquely Dangerous Tool': How Google's Data Can Help States Track Abortions*, POLITICO (July 18, 2022, 4:30 AM), https://www.politico.com/news/2022/07/18/google-data-states-track-abortions-00045906 [https://perma.cc/UFZ6-S8GA]; Taylor Hatmaker, *Congress Probes Period Tracking Apps and Data Brokers over Abortion Privacy Concerns*, TECHCRUNCH (July 8, 2022, 3:15 PM), https://techcrunch.com/2022/07/08/house-oversight-letter-abortion-period-apps-data-brokers/ [https://perma.cc/4UXA-CRDB].

reproductive health data they collect.[127] Recently, Facebook came under fire for cooperating with law enforcement and turning over messages between a Nebraska teen and her mother that proved instrumental in their prosecution for conducting an illegal abortion.[128]

Similar concerns have been raised over the prospect of law enforcement, in states where abortion is now illegal, using reverse keyword warrants to essentially conduct a dragnet search for anyone seeking information about obtaining an abortion or the "morning after" pill.[129] Moreover, since there are currently no tests for distinguishing a naturally-occurring miscarriage early in a pregnancy from a medication-induced abortion, search histories and digital evidence would be particularly sought after by law enforcement seeking to prosecute women and their doctors.[130] While there is movement in some state legislatures and courts to quash these unfair practices, nothing currently prevents law enforcement from using reverse keyword warrants in this capacity.[131]

C. Current Legal Status of Reverse Warrants and Reverse Keyword Warrants

This section addresses the legal status of reverse keyword warrants, beginning with a summary of two recent cases in which the analogous geofence warrants were found unconstitutional. It then discusses *People v. Seymour*, the first case to challenge the constitutionality of reverse keyword warrants. Finally, this section describes legislation in New York

---

[127] Kristin Poli, *The Most Popular Period-Tracking Apps, Ranked by Data Privacy*, WIRED (July 20, 2022, 7:00 AM), https://www.wired.com/story/period-tracking-apps-flo-clue-stardust-ranked-data-privacy/ [https://perma.cc/5WYK-7K2E].

[128] Naomi Nix & Elizabeth Dwoskin, *Search Warrants for Abortion Data Leave Tech Companies Few Options*, THE WASHINGTON POST, https://www.washingtonpost.com/technology/2022/08/12/Nebraska-abortion-case-facebook/ [https://perma.cc/S6HD-4XBN] (Aug. 12, 2022, 3:15 PM).

[129] Schuppe, *supra* note 12.

[130] *Will a Doctor Be Able to Tell If You've Taken Abortion Pills?*, WOMEN HELP (Sept. 23, 2019), https://womenhelp.org/en/page/1093/will-a-doctor-be-able-to-tell-if-you-ve-taken-abortion-pills [https://perma.cc/KJL8-LM36].

[131] *See* Cyrus Farivar, *Abortion Rights, Privacy Activists Push for California Ban on 'Digital Dragnet' Warrants,* FORBES (May 2, 2023, 6:00 AM), https://www.forbes.com/sites/cyrusfarivar/2023/05/02/abortion-rights-privacy-activists-push-for-california-ban-on-digital-dragnet-warrants/?sh=1c262d47bfc6 [https://perma.cc/X9XX-58V6].

and California that tried to prohibit the use of geofence and reverse keyword warrants.

1. Reverse Warrant Jurisprudence Generally

Currently, the preeminent federal case addressing a reverse warrant is a 2022 Virginia District Court case, *United States v. Chatrie*.[132] In *Chatrie* (discussed further *infra)*, law enforcement investigating a robbery at the Call Federal Credit Union obtained a geofence warrant to identify cell phone users within a 150-meter radius of the credit union an hour before and an hour after the crime.[133] The Court held this warrant was unconstitutional because it lacked particularized probable cause. It stated that, "warrants, like this one, that authorize the search of every person within an area must establish probable cause to search every one of those persons."[134]

Chatrie's analysis drew extensively on the Illinois District Court's 2020 opinion*, In re Search of Info. Stored at Premises Controlled by Google*. In this case, the district court denied the Government's request for a geofence warrant encompassing two locations during a forty-five minute window when they believed an unknown individual had stolen and shipped prescription drugs.[135] In denying the warrant, the Court reasoned

> [I]f the government can identify that wrongdoer only by sifting through the identities of unknown innocent persons without probable cause and in a manner that allows officials to rummage where they please in order to see what turns up, even if they have reason to believe something will turn up, a federal court in the United States of America should not permit the intrusion. Nowhere in

---

[132] Cullen Seltzer, *Google Knows Where You've Been. Should It Tell the Police?*, SLATE (May 16, 2022, 11:04 AM), https://slate.com/technology/2022/05/google-geofence-warrants-chatrie-location-tracking.html [https://perma.cc/C6G8-LMMZ]; *see generally* United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022).

[133] *Chatrie*, 590 F. Supp. 3d at 918–19.

[134] *Id.* at 927.

[135] *In re* Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 732–33 (N.D. Ill. 2020).

> Fourth Amendment jurisprudence has the end been held to justify unconstitutional means.[136]

Shortly after the decision in *Chatrie*, a California Court found a geofence warrant unconstitutional on similar grounds.[137] In *People v. Dawes*, law enforcement investigating a burglary obtained a geofence warrant to identify any cell phone users within an area loosely surrounding the victim's home within three time periods.[138] The Court held the warrant violated the particularity requirement of the Fourth Amendment, because it "did not narrowly identify 'the place to be searched'…rendering it overly broad in scope."[139]

While these cases do not speak to reverse keyword warrants, they address a highly analogous technology with similar constitutional ramifications and represent a potential changing tide in the legality of these technologically exploitative warrants.

2. First Constitutional Challenge

Despite being used as early as 2017, reverse keyword warrants faced their first constitutional challenge in the 2020 Colorado case, *People v. Seymour*.[140] In *Seymour*, law enforcement investigating an arson that killed five members of a Denver family found themselves with few leads other than a grainy surveillance video of three people in masks.[141] In an effort to identify the masked suspects, they used a series of increasingly broad warrants including cell tower dumps (which provided information on over a thousand people), a cell-site simulator (also known as a Stingray), two

---

[136] *Id.* at 757.

[137] *See generally* Order Granting Motion to Suppress Geofence Warrant, People v. Dawes, No. 19002022 (Super. Ct. Cal. Sept. 30, 2022), https://www.eff.org/files/2022/10/06/dawes_order_granting_mts.pdf [https://perma.cc/XP8H-GS8Q].

[138] *Id.* at 14–17.

[139] *Id.* at 39.

[140] Albert Fox Cahn & Julian Melendi, *The New Way Police Could Use Your Google Searches Against You*, SLATE (Aug. 1, 2022, 2:18 PM), https://slate.com/technology/2022/08/keyword-search-warrants-colorado-roe.html [https://perma.cc/GHK5-E97C].

[141] Janet Oravetz, *$40,000 Reward Offered After Denver Fire that Killed 5 Family Members*, 9NEWS, https://www.9news.com/article/news/crime/true-crime/diol-family/truckee-fire-arson-reward-increase-family-killed/73-ead32c99-2a87-4306-8a11-31c07cd25702 [https://perma.cc/6N4D-4QD9] (Sept. 9, 2020, 4:44PM).

geofence warrants, a warrant for Fog Reveal to query its aggregate location data, and three reverse keyword warrants.[142] Prior to the third reverse keyword warrant, authorities obtained almost two dozen warrants without identifying a suspect.[143]

Although authorities had to rework the first two warrants to comport with Google's format requirements and policies, the third warrant returned 61 queries belonging to about nine people.[144] Of these, "38 were associated with Colorado; 2 were associated with Illinois; and 21 were blank."[145] Additionally, while the reverse keyword warrant requested information on users who searched for nine variations of the arson's address, only five of the returned queries were one of the specified variations.[146]

Ultimately, authorities traced one of the IP addresses to the defendant, 16-year-old Gavin Seymour, who was charged with several offenses including first-degree murder.[147] Seymour's attorney moved to suppress the evidence obtained using the reverse keyword warrant, arguing that the warrant lacked particularity and sufficient probable cause.[148] However, the trial Court dismissed the motion.[149]

In January of 2023, the Colorado Supreme Court announced it would review the trial Court's decision to admit the keyword evidence.[150] Oral arguments took place on May 4th, 2023.[151]

---

[142] Motion to Suppress, *supra* note 31, ¶¶ 8–13.

[143] *Id.* ¶ 9.

[144] *Id.* ¶ 21, 25, 29, 31.

[145] *Id.* ¶ 29.

[146] *Id.* ¶ 30.

[147] *Id.* ¶ 34–35.

[148] *Id.* ¶ 7.

[149] Shelly Bradbury, *Green Valley Ranch Arson Suspects Signal They May Take Plea Deals After Judge Upholds Google Keyword Warrant*, THE DENVER POST, https://www.denverpost.com/2022/11/16/green-valley-ranch-arson-diol-google-bui-seymour/ [https://perma.cc/SG2H-33GZ] (Nov. 16, 2022, 5:48 PM).

[150] Jessica Seaman, *Colorado Supreme Court to Review Denver Police's Use of "Digital Dragnet" in Deadly Green Valley Ranch Arson Case*, THE DENVER POST, https://www.denverpost.com/2023/01/20/denver-police-reverse-keyword-search-colorado-supreme-court/ [https://perma.cc/F79V-2UXC] (Jan. 20, 2023, 5:17 PM).

[151] Shelly Bradbury, *Colorado Supreme Court Hears First-of-Its-Kind Challenge to Police's Use of Google Search Terms to ID Murder Suspects*, GREELEY TRIBUNE (May 5,

(*continued*)

On October 16th, 2023, the Court released its 5-2 decision.[152] It began by explaining that Seymour had a reasonable expectation of privacy in his Google search history under the Colorado constitution—which provides greater privacy guarantees than the United States Constitution—and a constitutionally protected possessory interest in his search history under the Colorado and United States constitutions.[153] The Court additionally found that the reverse keyword warrant was sufficiently particularized.[154] In drawing this conclusion it emphasized the fact that "[n]o human, let alone any law enforcement official, saw information falling outside the warrant's narrow search parameters[,]" noting that, "[p]roperly read, the warrant authorized a search for only nine specified keywords. Google may have produced more records than requested, but that issue is for Google and its users to resolve."[155] Finally, the Court assumed without deciding that the warrant lacked probable cause, ultimately holding that the evidence should be admitted under the good faith exception to the exclusionary rule.[156] However, the Colorado Supreme Court qualified its holding, explaining that

> In reaching these conclusions, we make no broad proclamation about the propriety of reverse-keyword warrants. As is often true when we examine what is reasonable under the search-and-seizure provisions of the federal and state constitutions, much is fact-dependent. Our finding of good faith today neither condones nor condemns all such warrants in the future. If dystopian problems emerge, as some fear, the courts stand ready to hear argument regarding how we should rein in law enforcement's use of rapidly advancing technology. Today, we proceed incrementally based on the facts before us.[157]

2023, 6:30 AM), https://www.greeleytribune.com/2023/05/05/google-reverse-keyword-search-warrant-colorado-supreme-court-arguments/ [https://perma.cc/5C9F-8QFX].

[152] *See* People v. Seymour, 536 P.3d 1260 (Colo. 2023).

[153] *Id.* at 1267, 1272.

[154] *Id.* at 1276.

[155] *Id.* at 1276–78.

[156] *Id.* at 1278–80.

[157] *Id.* at 1268.

The Colorado Supreme Court's decision to rule narrowly on the facts of Seymour, rather than addressing the constitutionality of reverse keyword warrants as a practice has drawn criticism from civil rights organizations and journalists watching the case.[158] In her dissenting opinion, Justice Márquez raised similar alarms, stating "I fear that by upholding this practice, the majority's ruling today gives constitutional cover to law enforcement seeking unprecedented access to the private lives of individuals not just in Colorado, but across the globe. And I fear that today's decision invites courts nationwide to do the same."[159]

Ultimately, the Colorado Supreme Court's decision leaves reverse warrant jurisprudence nearly as ambiguous as before Seymour was granted certiorari.[160] It will be left to other state and federal courts or legislators to take up the issue.[161]

---

[158] *See, e.g.* Jennifer Lynch & Andrew Crocker, *Colorado Supreme Court Upholds Keyword Search Warrant*, EFF DEEPLINKS BLOG (Oct. 16, 2023), https://www.eff.org/deeplinks/2023/10/colorado-supreme-court-upholds-keyword-search-warrant [https://perma.cc/WX48-V3U9] ("If the majority had truly engaged with the deep constitutional issues presented by this keyword warrant, it would have found, as the three-justices dissenting on this point did, that keyword warrants 'are tantamount to a high-tech version of the reviled "general warrants…"'"); *Colorado Supreme Court Condones Law Enforcement Use of Dangerous Reverse Keyword Warrant*, ELEC. PRIV. INFO. CTR.(Oct. 20, 2023), https://epic.org/colorado-supreme-court-condones-law-enforcement-use-of-dangerous-reverse-keyword-warrant/ [https://perma.cc/99VR-43ZB] ("While the Colorado Supreme Court addressed some issues…it declined to decide whether the warrant was supported by probable cause or constitutional because it said the police obtained the warrant in good faith…This represents a missed opportunity to rein in a new, dangerous police ability."); Mack DeGeurin, *'Invasive' Google Keyword Search Warrants Get Court Greenlight. Here's Everything You Need to Know*, Gizmodo (Oct. 20, 2023), https://gizmodo.com/reverse-keyword-search-warrants-explainer-colorado-1850945867 [https://perma.cc/23AG-HNDV] ("Despite pressure from the legal community to weigh in, the court threw up its hands and said it neither condoned nor condemned the practice. Future abuses of the warrant that may occur, they said, were a topic for another day.").

[159] Seymour, 536 P.3d at 1291(Márquez, J., dissenting).

[160] *See* Shelly Bradbury, *Colorado Supreme Court Upholds Controversial Google Search Warrant in Deadly Green Valley Ranch Arson Case*, THE DENVER POST (Oct. 16, 2023, 4:41 PM), https://www.denverpost.com/2023/10/16/colorado-supreme-court-reverse-keyword-search-google-green-valley-ranch-arson/ [https://perma.cc/Q69K-2GBY] ("The

(*continued*)

3. Legislative Response

While the Colorado Supreme Court is the first Supreme Court in the United States to address the constitutionality of reverse keyword warrants, legislation has been introduced around the country seeking to curtail the use of reverse warrants.[162] In New York, The Reverse Location Search Prohibition Act has been introduced during each legislative session since 2020.[163] This bill would amend the state's criminal procedure law to prohibit

> the search, with or without a warrant, of geolocation and keyword data of a group of people who are under no individual suspicion of having committed a crime, but rather are defined by having been at a given location at a given time or searched particular words, phrases, character strings, or websites.[164]

Although the bill failed to pass before the legislature adjourned for the year, support is growing, and it will likely be reintroduced in the 2024 session.[165] This increased concern for digital incursions on privacy is evidenced by Fiscal Bill A.3007C/S.4007, which was signed into law by New York Governor, Kathy Hochul in May of 2023.[166] While Fiscal Bill A.3007C/S.4007 does not address reverse keyword warrants, it prohibits

---

ruling essentially leaves open the issue of whether reverse keyword search warrants are constitutionally acceptable…").

[161] *See* DeGeurin, *supra* note 158.

[162] Lynch & Crocker, *supra* note 14; Albert Fox Cahn & Nina Loshkajian, *The Police Surveillance Tool Too Dangerous to Ignore*, SLATE (June 5, 2023, 3:57 PM), https://slate.com/technology/2023/06/geofence-keyword-warrant-police-surveillance-new-york-law.html [https://perma.cc/R9HM-LVZN] ("New York's proposal is being replicated across the country, including in traditionally conservative states like Missouri and Utah.").

[163] Cahn & Loshkajian, *supra* note 162.

[164] S. 217, 2023–2024 Leg., Reg. Sess. (N.Y. 2023).

[165] Cahn & Loshkajian, *supra* note162.

[166] *New York Passes Bill that Includes Prohibition on Geofences at Healthcare Facilities*, ABA HEALTH L. SECTION NEWS (June 2, 2023), https://www.americanbar.org/groups/health_law/section-news/2023/june/new-york-passes-bill-that-includes-prohibition-on-geofences-at-healthcare-facilities/ [https://perma.cc/G6W7-4LL2].

persons and entities from erecting a geofence around healthcare facilities.[167]

In 2023, California Assemblywoman, Mia Bonita introduced a piece of legislation similar to The Reverse Location Search Prohibition Act.[168] In a statement about the legislation Bonita stated the bill was specifically introduced to protect the privacy of people seeking abortions or gender affirming care from "unconstitutional searches of their data."[169] While the bill passed assembly, opposition from law enforcement groups slowed its progress.[170] In an effort to get A.B. 793 passed before the end of the state's legislative session, the bill's sponsor agreed to limit its scope to reverse warrants targeting those seeking reproductive or gender-affirming care.[171] Although this does not fully address the dangers presented by reverse warrants, it would be a start toward curtailing them.[172]

Until the Court chooses to take up the issue of reverse keyword warrants, legislation like that proposed in New York and California remains the most promising solution for mitigating the threats posed by these types of warrants.[173]

III. LAW & ARGUMENT

Given the current lack of precedent addressing the constitutionality of reverse keyword warrants, it is necessary to begin with the foundational principles of Fourth Amendment analysis. Therefore, this section first uses

---

[167] *Id.*

[168] Tonya Riley, *California Lawmaker Seeks to End to 'Reverse Warrants' that Could Pinpoint Abortion Seekers*, CYBERSCOOP (Feb. 13, 2023), https://cyberscoop.com/california-lawmaker-reverse-warrants-abortion/ [https://perma.cc/QVJ6-SDS6].

[169] *California Bill Will Protect People Seeking Abortion and Gender-Affirming Care from Dragnet Digital Surveillance*, CAL. STATE ASSEMB. DEMOCRATIC CAUCUS (Feb. 13, 2023), https://a18.asmdc.org/press-releases/20230213-california-bill-will-protect-people-seeking-abortion-and-gender-affirming [https://perma.cc/75K4-DNXF].

[170] Titus Wu, *Abortion Fears Spur Reverse Search Warrant Bill in California*, BLOOMBERG L. (June 14, 2023, 5:00 AM), https://news.bloomberglaw.com/in-house-counsel/abortion-fears-spur-reverse-search-warrant-bill-in-california [https://perma.cc/JWJ8-P924].

[171] *Id.*

[172] *Id.*

[173] Winters, *supra* note 37, at 1412–13.

the Supreme Court's holding in *Carpenter v. United States* to argue obtaining users' Google history is a search under the Fourth Amendment (requiring a warrant) and the third-party doctrine exception does not apply. After discussing the necessity of a warrant, it then addresses how reverse keyword warrants fail to meet the technical warrant requirements of the Fourth Amendment given their similarity to historic general warrants and failure to meet the particularity requirement.

A. A Keyword Search Is a Fourth Amendment Search of Google Users

In *Katz v. United States*, the Supreme Court held a Fourth Amendment search occurred when FBI agents attached an electronic eavesdropping device to a public phone booth so they could listen to Mr. Katz's conversation.[174] In his concurrence, Justice Harlan established a two-prong test for when a search has occurred under the Fourth Amendment: "a person [must] have exhibited an actual (subjective) expectation of privacy and . . . the expectation be one that society is prepared to recognize as 'reasonable.'"[175]

1. A Subjective Expectation of Privacy

Technology has progressed substantially since Katz's telephone phone booth call and, along with it, people's expectations of privacy.[176] While it is not yet possible to scan an individual's thoughts, a user's search history is a close approximation.[177] One need only look at a list of the top searches or autocomplete suggestions—which Google generates from actual searches—to see how personal an individual's searches are.[178] Many involve health, sexuality, and other private topics a person would be unlikely to speak about with those close to them, let alone the public at

---

[174] 389 U.S. 347, 348 (1967).

[175] *Id.* at 361 (Harlan, J., concurring).

[176] *See generally* MARY MADDEN & LEE RAINIE, AMERICANS' ATTITUDES ABOUT PRIVACY, SECURITY AND SURVEILLANCE, PEW RSCH. CTR. (May 20, 2015), https://www.pewresearch.org/wp-content/uploads/sites/9/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf [https://perma.cc/EBR2-XAPQ].

[177] Amicus Brief Supporting Defendant, *supra* note 32, at 1–2.

[178] *How Google Autocomplete Predictions Work*, GOOGLE SEARCH HELP, https://support.google.com/websearch/answer/7368877?hl=en [https://perma.cc/74MZ-XR3E].

large.[179] Just as people feel comfortable sharing health information with a doctor or psychiatrist or seeking advice from a lawyer due to their duties of confidentiality, people are similarly candid with search engines because they do not believe others will look at their search history.[180] Thus, people display a subjective expectation of privacy in their searches.

2. An Expectation of Privacy that Society is Prepared to Recognize as Reasonable

Google processes 8.5 billion searches each day.[181] Searching the Internet for relevant content is integral to people's ability to conduct business, complete schoolwork, and manage personal affairs.[182] Considering the number of people potentially impacted by intrusive reverse keyword warrants, the right to privacy in one's search history is likely one that society is prepared to recognize.[183]

While the Supreme Court has not yet addressed reverse keyword warrants, its recent line of Fourth Amendment search precedent shows a growing acknowledgment of the threat to privacy posed by electronic means of surveillance. For instance, in the 2012 case *United States v. Jones* the Court held a Fourth Amendment search took place when federal agents investigating narcotics distribution attached a GPS to the defendant's wife's vehicle and tracked its movements around the clock for four weeks.[184]

While Justice Scalia's majority opinion reached this conclusion using a common law trespass analysis, Justice Sotomayor's concurrence examined the privacy interests implicated by GPS technology.[185] She noted that, "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[186] She went on to state that in determining whether there is a reasonable societal expectation of privacy, she would, "ask whether people reasonably expect

---

[179] Amicus Brief Supporting Defendant, *supra* note 32, at 1–2.

[180] *See* Motion to Suppress, *supra* note 31, ¶ 42.

[181] Amadeo, *supra* note 40.

[182] Lynch & Crocker, *supra* note 14.

[183] *See* Motion to Suppress, *supra* note 31, ¶ 97.

[184] 565 U.S. 400, 403–05 (2012).

[185] *See id.* at 413–15 (Sotomayor, J., concurring).

[186] *Id.* at 415.

that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[187]

Sotomayor's proposed analysis strongly influenced the Court's opinion in the 2018 case *Carpenter v. United States*.[188] In *Carpenter,* FBI agents investigating a series of robberies obtained a court order for 127 days of historic cell tower location data to link Carpenter to locations where crimes took place.[189] The data returned by Carpenter's wireless carrier amounted to "12,898 location points cataloging Carpenter's movements—an average of 101 data points per day."[190] The Court held that an individual has an expectation of privacy in their historic location data, and, thus, the government's actions were a Fourth Amendment search.[191] It reasoned that "the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[192] These location records "hold for many Americans the 'privacies of life.'"[193]

Reverse keyword warrants can provide an even more intimate window into people's lives than GPS or cell tower location data. While the *Jones* concurrence and *Carpenter* discuss what can be inferred from an individual's movements, no inference needs to be made regarding a user's search history.[194] The user's most intimate thoughts and questions are laid

---

[187] *Id.* at 416.

[188] Mark Joseph Stern, *Sotomayor, Fourth Amendment Visionary*, SLATE (June 24, 2018, 5:56 PM), https://slate.com/news-and-politics/2018/06/in-carpenter-v-united-states-the-supreme-court-vindicates-justice-sonia-sotomayors-theory-of-digital-privacy.html [https://perma.cc/WY2A-A5L5].

[189] Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

[190] *Id.*

[191] *Id.* at 2220.

[192] *Id.*

[193] *Id.* at 2217 (first quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring); then quoting Riley v. California, 573 U.S. 373, 403 (2014)).

[194] United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."); (*continued*)

bare in plain text. Because the types of keywords that can be sought in a reverse keyword warrant are limited only by the ability of an officer to justify its connection to the case being investigated, law enforcement could conceivably request information on users who searched for the address of an abortion clinic, mental health services, particular pornography, or political tracts.[195] While *Jones* and *Carpenter* speak of the intrusive potential of aggregate location data, any one of the aforementioned searches on its own would reveal the "privacies of life."[196]

The intimate nature of search histories can be illustrated by the 2006 America Online (AOL) search log release in which the company published the search histories of 500,000 users over a three-month period.[197] While AOL replaced the individuals' usernames with numbers before releasing the data, the highly personal nature of the information allowed users to be quickly identified.[198] Within days of the release, 62-year-old Thelma Arnold became the first searcher identified by name.[199] Many search histories contained queries relating to medical issues, pornography, and other subjects that a person would not likely reveal to the public at large.[200] Several users whose information was released by AOL brought a class action lawsuit; the search engine ultimately settled.[201]

Carpenter, 138 S. Ct. at 2218 ("A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales.").

[195] *See* Amicus Brief Supporting Defendant, *supra* note 32, at 4–5.

[196] *Carpenter*, 138 S. Ct. at 2212–13 (quoting Riley v. California, 573 U.S. 373, 403 (2014)).

[197] Nate Anderson, *AOL Releases Search Data on 500,000 Users (Updated*), ARS TECHNICA (Aug. 7, 2006, 11:39 AM), https://arstechnica.com/uncategorized/2006/08/7433/ [https://perma.cc/KE9B-CLH8].

[198] Michael Barbaro & Tom Zeller Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES (Aug. 9, 2003), https://www.nytimes.com/2006/08/09/technology/09aol.html [https://perma.cc/7UX5-TDPJ]

[199] *Id.*

[200] *Id.*

[201] Paul Bond, *Court Grants Final Approval to Class Action Settlement over AOL's 2006 Anonymization Failure; Big Data Precursor Settles for Millions*, REEDSMITH:TECH. L. DISPATCH (May 30, 2013), https://www.technologylawdispatch.com/2013/05/big-data/court-grants-final-approval-to-class-action-settlement-over-aols-2006-anonymization-failure-big-data-precursor-settles-for-millions/ [https://perma.cc/L4R4-6QSV].

3. Third-Party Doctrine Does Not Apply to Reverse Keyword Searches

Generally, the third-party doctrine dictates that a person does not have a reasonable expectation of privacy in that which he voluntarily reveals to a third-party.[202] Therefore, the government is not required to obtain a warrant and any examination of this information does not constitute a Fourth Amendment search.[203]

Given how most digital life is mediated through Internet service providers, cellular service carriers, and websites–all of which collect data on their users–the third-party doctrine has been interpreted to mean there cannot be a reasonable expectation of privacy in one's digital information.[204] Recent cases like *Jones* and *Carpenter*, however, have called this interpretation into question.[205] Thus, to establish that reverse keyword searches implicate the Fourth Amendment and require a valid warrant, it is necessary to use these precedents to show the third-party doctrine does not apply to search history data.

This section will begin by discussing the cases that established the third-party doctrine and how the Court's view has changed in recent years. It will then apply these new rules to searches of keyword data.

a. Third-Party Doctrine Precedent

The Court established the third-party doctrine in its 1976 opinion in *United States v. Miller*.[206] In *Miller*, the Court held a defendant did not have a reasonable expectation of privacy in his banking records because he

---

[202] Clifton B. Parker, *Key Privacy Doctrine Needs Updating Due to Technology, Stanford Law Professor Says*, STAN. NEWS (June 9, 2015), https://news.stanford.edu/2015/06/09/privacy-third-party-060915/ [https://perma.cc/G9DX-QAJ4].

[203] *Id.*

[204] Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SEC. L. & POL'Y 247, 268–69 (2016).

[205] Orin Kerr & Greg Nojeim, *The Data Question: Should the Third-Party Records Doctrine Be Revisited?*, A.B.A. J. (Aug. 1, 2012, 9:20 AM), https://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited [https://perma.cc/M8P2-8T75]; Orin Kerr, *Understanding the Supreme Court's* Carpenter *Decision*, LAWFARE (June 22, 2018, 1:18 PM), https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision [https://perma.cc/LZA4-7BFG].

[206] RICHARD M. THOMPSON II, CONG. RSCH. SERV., R43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE 9 (2014).

voluntarily gave them to his bank.[207] It reasoned that "[t]he checks are not confidential communications but negotiable instruments to be used in commercial transactions. All the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[208]

Smith v. Maryland elaborated on this doctrine. In *Smith*, the defendant moved to suppress evidence collected when his telephone company installed a pen register on his phone at the request of law enforcement.[209] The Court held the defendant lacked a reasonable expectation of privacy in the phone numbers he dialed because he voluntarily turned the information over to a third party (the telephone company).[210] The Court also expressed doubt that "people in general entertain any actual expectation of privacy in the numbers they dial."[211]

While the Court in *Jones* decided the collection of GPS data constituted a Fourth Amendment search on the basis of the physical intrusion on the defendant's vehicle, in her concurrence, Justice Sotomayor questioned the applicability of these earlier third-party doctrine cases to the modern era, stating that the 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."[212] She went on to suggest society would recognize this expectation of privacy as reasonable because people would be unlikely to "accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year."[213] She concluded that

> Whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the

---

[207] *Id.* at 10.

[208] United States v. Miller, 425 U.S. 435, 442 (1976).

[209] THOMPSON II, *supra* note 206, at 11.

[210] *Id.*

[211] Smith v. Maryland, 442 U.S. 735, 742 (1979).

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

[213] *Id.* at 418.

> public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[214]

The third-party doctrine remained largely intact for 42 years, until the Court handed down its landmark opinion in *Carpenter*.[215] While *Carpenter* did not overturn *Miller* or *Smith*, the Court declined to apply the third-party doctrine to historical cell tower location data despite the data being held by the defendant's cellular service provider (a third-party).[216] It reasoned that "[i]n light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection."[217]

While the implications of *Carpenter* are still being explored, it provides at least one situation in which the third-party doctrine does not apply to digital information and a set of attributes that may be applied to other information technologies in evaluating whether this exception applies.[218]

---

[214] *Id.*

[215] Steven J. Arango, *The Third-Party Doctrine in the Wake of a "Seismic Shift,"* ABA (June 13, 2019), https://www.americanbar.org/groups/litigation/committees/privacy-data-security/practice/2019/third-party-doctrine-wake-of-seismic-shift/?login [https://perma.cc/CZ2Y-Z2QW].

[216] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

[217] *Id.* at 2223.

[218] Matthew Tokson, *The Impact of* Carpenter v. United States *in the Lower Courts and the Emerging* Carpenter *Test*, LAWFARE (Nov. 3, 2021, 2:08 PM), https://www.lawfareblog.com/impact-carpenter-v-united-states-lower-courts-and-emerging-carpenter-test [https://perma.cc/XQT4-Q3R5]; *See Carpenter*, 138 S. Ct. at 2223 (2018) ("We decline to grant the state unrestricted access to a wireless carrier's database of physical location information. In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection.").

b. Application to Reverse Keyword Searches

At the time *Smith* and *Miller* were decided, computers were in their infancy.[219] The closest technology to the Internet was the Advanced Research Projects Agency's computer network, ARPANET, which allowed computers to send information between one another.[220] Unlike today's Internet, which is used by 93% of American adults, ARPANET was only available to academic and military researchers.[221] Few people could have predicted the role this technology would come to have in everyone's lives.[222]

A person's search history is fundamentally different from the banking documents in *Smith* or the phone numbers in *Miller*. While a user does employ the services a search engine to perform his query, as the Court noted in *Carpenter*, *Smith,* and *Miller* "did not rely solely on the act of sharing. Instead, they considered 'the nature of the particular documents sought' to determine whether 'there is a legitimate 'expectation of privacy' concerning their contents.'"[223] In both cases, the Court emphasized the limited information revealed by the documents in holding that their collection did not constitute a Fourth Amendment search.[224]

The information revealed by a person's search history is not limited, but rather "revealing of their most intimate and private thoughts, ideas, and concerns."[225] Like the cell tower location data in *Carpenter*, the

---

[219] *See A Short History of the Internet*, SCI. & MEDIA MUSEUM (Dec. 3, 2020), https://www.scienceandmediamuseum.org.uk/objects-and-stories/short-history-internet#what-is-packet-switching [https://perma.cc/E5DX-99JX].

[220] *See id.*

[221] *Internet/Broadband Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/internet-broadband/ [https://perma.cc/J7YD-EDYR] ("By 1973, 30 academic, military and research institutions had joined the network, connecting locations including Hawaii, Norway and the UK.").

[222] *See Carpenter*, 138 S. Ct. at 2217.

[223] *Id.* at 2219.

[224] *Id.* ("*Smith* pointed out the limited capabilities of a pen register; as explained in *Riley*, telephone call logs reveal little in the way of 'identifying information.' . . . *Miller* likewise noted that checks were 'not confidential communications but negotiable instruments to be used in commercial transactions.'").

[225] Amicus Brief Supporting Defendant, *supra* note 32, at 4.

retrospective nature of a person's Internet searches offers law enforcement access to otherwise unknowable information. While historic cell tower location data reveals where a person was in the past and along with it potentially private information, keyword data reveals in plain text a detailed chronical of what a person was thinking at a given time.[226]

Moreover, logging keyword data is inescapable in modern society. As the Court acknowledged in *Carpenter*, "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[227] The ability to use the Internet is one such service. In 2016, the United Nations acknowledged this when 193 member countries adopted a resolution stating the ability to use the Internet is a human right.[228]

Using the Internet would be wholly impractical without using a search engine as there are currently over a billion websites.[229] Without a search engine to index these websites, users would have to memorize the URLs for the hundreds of websites they use to carry out daily tasks or complete work, and it would be very difficult to discover new material and answer important questions.[230] Moreover, users would find it challenging to find material within a website as many use a search function to navigate various webpages.[231]

The collection of this data is inescapable because it is not practicable to use Google anonymously.[232] Although Google allows users to delete their search histories and turn off collection, this does not defeat an individual's reasonable expectation of privacy because Google still collects

---

[226] *See The Most Asked Questions on Google*, MONDOVO, https://www.mondovo.com/keywords/most-asked-questions-on-google [https://perma.cc/5HQZ-JLG6].

[227] *Carpenter*, 138 S. Ct. at 2220 (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

[228] Catherine Howell & Darrell M. West, *The Internet as a Human Right*, BROOKINGS INST. (Nov. 7, 2016), https://www.brookings.edu/blog/techtank/2016/11/07/the-internet-as-a-human-right/ [https://perma.cc/QT4C-6275].

[229] Lynch & Crocker, *supra* note 14; *February 2023 Web Server Survey*, NETCRAFT (Feb. 28, 2023), https://news.netcraft.com/archives/category/web-server-survey/ [https://perma.cc/TGS6-2MLP].

[230] Amicus Brief Supporting Defendant *supra* note 32, at 7–8.

[231] *Id.*

[232] *Id.* at 8.

the data.[233] Turning off the collection of search history data only "divorces that collection from other details in a user's account"; Google still collects data on anyone who uses the search engine and links it to their IP address.[234] While there are services like virtual private networks (VPNs), incognito browsers, or alternate search engines which promise improved privacy protections, these too fail to render the user anonymous.[235] Other services, like the Tor browser, are also imperfect and may be unworkable for the average Internet user because they require complex technical knowledge to properly implement.[236]

As Justice Sotomayor suggested in her *Jones* concurrence and the Court seemed to acknowledge in *Carpenter,* absolute secrecy is not the sole metric for whether an individual's expectation of privacy is reasonable.[237] Rather, it is the "deeply revealing nature of [the data], its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection. . . ."[238]

Thus, considering the Court's holding in *Carpenter*, Google's possession of the keyword data fails to diminish users' reasonable expectations of privacy. As such, a reverse keyword search is a search under the Fourth Amendment and requires a valid warrant.

---

[233] *Id.* at 7 ("[I]f users do not take active steps to delete their data, Google will likely have a record of everything they have ever searched for dating back years to when they first set up their Google account.").

[234] *Id.* at 7–8.

[235] Eric Griffith, *How to Completely Disappear from the Internet*, PC MAG. (Oct. 24, 2022), https://www.pcmag.com/how-to/how-to-stay-anonymous-online [https://perma.cc/F2JC-BZND].

[236] *Id.*

[237] United States v. Jones, 565 U.S. 400, 418 (2012) ("[W]hatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy."); Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) (quoting Riley v. California, 573 U.S. 373, 392 (2014) ("The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another. But the fact of 'diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely.' *Smith* and *Miller*, after all, did not rely solely on the act of sharing.").

[238] *Carpenter*, 138 S. Ct. at 2223.

B. Reverse Keyword Warrants Fail to Meet the Technical Warrant Requirements of The Fourth Amendment

The warrant clause of the Fourth Amendment states that "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."[239] This section will begin by discussing the historical origins of the Fourth Amendment and the similarities between reverse keyword warrants and the general warrants that The Framers of the Constitution sought to prohibit. It will then explore how reverse keyword warrants fail to meet the Fourth Amendment's particularity requirement.

1. Historical Basis of The Fourth Amendment

It is said that "[f]ew provisions of the Bill of Rights grew so directly out of the experience of the colonials as the Fourth Amendment."[240] In 1767, Parliament passed four acts collectively known as the Townsend Acts to maintain control over the American colonies.[241] The third of these acts authorized the use of writs of assistance to search for smuggled items.[242] Writs of assistance were essentially general warrants that allowed the holder to search any house whenever he pleased.[243] Their use was so widely despised that "[o]pposition to such searches was in fact one of the driving forces behind the Revolution itself."[244]

---

[239] U.S. CONST. amend. IV.

[240] *Historical Background on Fourth Amendment*, CONG. RSCH. SERV.: CONST. ANNOTATED, https://constitution.congress.gov/browse/essay/amdt4-2/ALDE_00013706/ [https://perma.cc/AJ6S-GQZ3].

[241] *Townshend Acts*, ENCYC. BRITANNICA, https://www.britannica.com/event/Townshend-Acts [https://perma.cc/TQK6-9H7V].

[242] *Id.*

[243] *Against Writs of Assistance (1761),* NAT'L CONST. CTR., https://constitutioncenter.org/the-constitution/historic-document-library/detail/james-otis-against-writs-of-assistance-february-24-1761 [https://perma.cc/7675-6EJ5] ("Agents would no longer need to obtain individual search warrants each time they sought to conduct a search, but instead could freely search vessels and homes without probable cause or express permission.").

[244] Riley v. California, 573 U.S. 373, 403 (2014).

While the passage of the Townsend Acts catalyzed widespread resistance to writs of assistance, they were in use even earlier.[245] In 1761, when the colonial government sought to renew the writs of assistance, it was challenged by a group of Boston merchants represented by a lawyer named James Otis.[246] In his arguments, Otis stated writs of assistance were "the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English lawbook."[247] A young John Adams was present for Otis' five-hour speech to the Court, and later said that "American Independence was then and there born . . . ."[248]

According to the Supreme Court, it is "familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment."[249] This is especially clear in the language of the warrant clause, which requires a warrant to "*particularly* describ[e] the place to be searched, and the persons or things to be seized."[250] The drafters of the Fourth Amendment wanted to prevent the use of arbitrary searches as a means of oppression and harassment.[251] By requiring authorities to establish probable cause as to a particular person or place and obtain approval for a warrant, the drafters hoped incursions on

---

[245] *Writ of Assistance*, ENCYC. BRITANNICA, https://www.britannica.com/topic/writ-of-assistance [https://perma.cc/Y9CR-HVVN] ("When similar warrants were expressly reauthorized by the Townshend Acts (1767), they were challenged for five years in every superior court in the 13 colonies and refused outright in 8 of them. Thus, writs of assistance became a major colonial grievance in the pre-Revolutionary period.").

[246] *Id.*

[247] Erick Trickey, *Why the Colonies' Most Galvanizing Patriot Never Became a Founding Father*, SMITHSONIAN MAG. (May 5, 2017), https://www.smithsonianmag.com/history/transformative-patriot-who-didnt-become-founding-father-180963166/ [https://perma.cc/PQQ5-NULB].

[248] *From John Adams to William Tudor, Sr., 29 March 1817*, NAT'L ARCHIVE, https://founders.archives.gov/documents/Adams/99-02-02-6735 [https://perma.cc/2KKA-CZTN].

[249] Payton v. New York, 445 U.S. 573, 584 (1980).

[250] U.S. CONST. amend. IV.

[251] *See* Frazelle & Gray, *supra* note 30 ("Under the authority of general warrants, the king's agents used the power to search and seize as a tool of oppression, targeting disfavored religious minorities and political opponents, such as those who published pamphlets criticizing the government.").

privacy would be limited and occur only when necessary.[252] These constitutional protections, however, can become lost amid the rapid emergence of new technologies and the Court's slow reaction to them.[253]

2. Reverse Keyword Warrants are General Warrants.

Reverse keyword warrants are tantamount to modern-day writs of assistance and do not satisfy the Fourth Amendment's particularity requirement.[254] Just as the colonial writs of assistance allowed authorities to search homes for contraband at will, reverse warrants, as illustrated by the facts of *Chatrie*, allow the police to obtain information about an unlimited number of people, despite most of those individuals having absolutely no nexus with criminal activity—let alone a nexus based upon probable cause.

In *Steele v. United States*, the Court held that to satisfy the particularity requirement, "[i]t was enough if the description is such that the officer with a search warrant can, with reasonable effort, ascertain and identify the place intended."[255] By their very nature, reverse keyword warrants do not specify a particular person whose Internet search history is to be examined: they specify only certain words or phrases.[256] To comply with these warrants, search engines must comb through over a billion users' information, the vast majority of whom will not and often could not have had anything to do with the criminal activity at issue.[257] For instance, in *People v. Seymour*, the arson occurred in Colorado.[258] The reverse keyword warrant, however, returned data on two people from Illinois who could not possibly have committed the crime because they were about 1,000 miles away.[259]

Reacting to Britain's use of general warrants, The Framers of the Constitution placed special emphasis on protecting the home from

---

[252] *See The Right to Be Secure: The Foundation of the Fourth Amendment*, INST. FOR JUST., https://ij.org/issues/ijs-project-on-the-4th-amendment/the-right-to-be-secure-the-foundation-of-the-fourth-amendment/ [https://perma.cc/3KFL-JCUH].

[253] *See* Baker & Gold, *supra* note 37.

[254] Motion to Suppress, *supra* note 31, ¶ 3.

[255] Steele v. United States, 267 U.S. 498, 503 (1925).

[256] *See* Motion to Suppress, *supra* note 31, ¶ 72.

[257] *Id.* ¶ 29.

[258] *Id.*

[259] *Id.*

unreasonable searches.[260] This emphasis was reasonable at a time when the home was a person's innermost sanctum that contained many–if not all–all–their papers and personal effects.[261] As more aspects of people's lives have moved online, probing a user's search history has the potential to reveal even more information about them than the contents of their home.[262] With the massive proliferation of websites offering free content, it is unlikely law enforcement would find a physical cache of erotica in a person's home, whereas, they could request information on users who had searched for pornographic material.[263] Similarly, modern subversive and political writing tends to be published on the Internet rather than in physical pamphlets, meaning a probe of search history would be more enlightening about an individual's political affiliations than a search of their home where they are unlikely to have physical copies of a given document.[264]

Moreover, in the colonial era, the number of houses that could be searched in a given period using a general warrant was limited by the time each search took and the amount of manpower available to conduct the search.[265] Reverse keyword warrants are not limited by such physical practicalities and frequently require the search engine to probe all its users' data to compile a response to the request.[266] This is essentially the equivalent of police investigating a shooting by simultaneously searching every house in the United States for a .45 pistol because that is the weapon they believe was used in the crime. In such a search, many innocent people would have their privacy violated and a portion of the 30% of Americans who own one or more guns would find themselves implicated in a crime many could not possibly have committed.[267]

---

[260] Thomas P. Crocker, *The Fourth Amendment at Home*, 96 IND. L.J. 167, 168–179 (2020).

[261] *See id.* at 210–11.

[262] Motion to Suppress, *supra* note 31, ¶ 4.

[263] *See* Louis Theroux, *How the Internet Killed Porn*, THE GUARDIAN, https://www.theguardian.com/culture/2012/jun/05/how-internet-killed-porn [https://perma.cc/MK79-B4A2] (June 15, 2012).

[264] *See* Motion to Suppress, *supra* note 31, ¶¶ 83–84.

[265] Amicus Brief Supporting Defendant, *supra* note 32, at 14.

[266] Motion to Suppress *supra* note 31, ¶ 29.

[267] KIM PARKER ET AL., AMERICA'S COMPLEX RELATIONSHIP WITH GUNS, PEW RSCH. CTR. (June 22, 2017), https://www.pewresearch.org/social-trends/wp-content/

(*continued*)

3. Reverse Keyword Warrants Lack Particularized Probable Cause

In *Illinois v. Gates,* the Court established the standard for probable cause in the context of a search.[268] It adopted a totality-of-the-circumstances analysis and held that an issuing magistrate need only determine whether "there is a fair probability that contraband or evidence of a crime will be found in a particular place."[269]

In *Ybarra v. Illinois* (discussed further *infra*) the Court held that the search of a patron in a tavern where authorities had a warrant to search the premises and bartender was unconstitutional because a "search or seizure of a person must be supported by probable cause particularized with respect to that person."[270]

In 2022, the Virginia District Court applied this precedent to geofence warrants in *United States v. Chatrie*, holding that a geofence warrant seeking information on all the cell phones logged into Google within a 150-meter radius of a bank robbery from one hour before the robbery to one hour afterward was unconstitutional.[271] It reasoned the warrant lacked particularity because "warrants, like this one, that authorize the search of every person within a particular area must establish probable cause to search every one of those persons."[272] While geofence warrants seek the information of all Google users with 'Location History' enabled on their devices in an area at a given time, rather than individuals who searched for a particular keyword, an analogy can be drawn to reverse keyword warrants.[273]

Reverse keyword warrants–like geofence warrants–are unlike any other type of traditional warrant. When conducting a traditional search, authorities begin with a particular suspect or location that they believe may have evidence of the crime they are investigating.[274] Reverse warrants

---

uploads/sites/3/2017/06/Guns-Report-FOR-WEBSITE-PDF-6-21.pdf [https://perma.cc/4AVX-J2WR].

[268] 462 U.S. 213, 238 (1983).

[269] *Id.*

[270] 444 U.S. 85 at 90–91 (1979).

[271] 590 F. Supp. 3d 901, 918–19 (E.D. Va. 2022).

[272] *Id.* at 927.

[273] Motion to Suppress, *supra* note 31, ¶ 11.

[274] *Id.* ¶ 80.

invert this.[275] They use a broad, dragnet search of many individuals to develop more particular suspicions.[276] This practice patently goes against the holdings of multiple Circuits that a warrant must be "no broader than the probable cause on which it is based."[277]

When Google responds to a reverse keyword search warrant, it must sift through the search histories of over a billion users.[278] It is functionally impossible for law enforcement to have probable cause to believe that each of the individuals whose privacy is invaded could be involved in the crime.[279] Particularly when so many are outside of the geographic boundaries in which it would even be feasible for them to have been involved.[280]

Further, reverse keyword warrants tend to rely on what is fundamentally a hunch.[281] The Court has long held that probable cause and even the lower standard of reasonable suspicion must not be based on an officer's "inchoate and unparticularized suspicion or 'hunch,' " but rather "the specific reasonable inferences which he is entitled to draw from the facts in light of his experience."[282] Courts have held that in order to satisfy the probable cause requirement for a valid warrant there must be "a 'link' between the evidence and the location of the search."[283]

In the absence of a particular suspect or facts tending to suggest the perpetrator of a crime engaged in a query, authorities are simply guessing a query using the particular keyword was made. This is the quintessential "fishing expedition" the particularity requirement is intended to prevent law enforcement from engaging in.

---

[275] *See Id.* ¶ 6.

[276] *Id.* ¶ 1.

[277] *Chatrie*, 590 F. Supp. 3d at 928 (E.D. Va. 2022) (quoting United States v. Hurwitz, 459 F.3d 463, 473 (4th Cir. 2006)); *see also* United States v. Zimmerman, 277 F.3d 426, 432 (3d Cir. 2002); United States v. Weber, 923 F.2d 1338, 1342 (9th Cir. 1990).

[278] Motion to Suppress, *supra* note 31, ¶ 1.

[279] Amicus Brief Supporting Defendant, *supra* note 32, at 13.

[280] *Id.*

[281] *Id.* at 2.

[282] Terry v. Ohio, 392 U.S. 1, 27 (1968).

[283] *Probable Cause to Search: The "Nexus" Requirement*, POINT OF VIEW (Alameda Cnty. Dist. Att'y's Off., Oakland, Cal.), Spring/Summer 2021, at 1, https://le.alcoda.org/publications/point_of_view/files/AAZZ_SS21_NEXUS.pdf [https://perma.cc/P3KY-W7GX].

For instance, in the affidavit for the Austin serial bombing case (discussed *supra*) an agent justified the need to identify any user who searched an explosives-related term within a three-month period by stating there was probable cause because "individuals who searched for these specific terms during this time period will help law enforcement to identify persons who may have knowledge about the bombings."[284] There were no facts, however, suggesting the person who carried out the bombings made any of those searches beyond the affiant's assertion that "it is common to utilize search applications such as Google Search and YouTube to research how to assemble and detonate explosive devices," and that "an individual that utilized the search terms . . . would find webpages and YouTube videos helpful in assembling the explosive devices under investigation."[285]

By the same logic, law enforcement could use such warrants to compel Amazon.com, or even libraries, to disclose the purchasing or borrowing habits of anyone who reads or buys particular books. Surely the lack of any information to link book buyers with a crime would shield them from the prying eyes of law enforcement. The same should hold true of their search histories.

Similarly, in *Seymour,* law enforcement justified its reverse keyword warrant by speculating that given the "personal nature of this offense" and "the amount of planning that likely went into a coordinated attack such as this one," the perpetrator must have searched the victims' address prior to the arson.[286] This was mainly speculation as law enforcement at that time had no suspects and no clear theory of the case.[287] Their primary piece of evidence was a grainy surveillance video of three masked individuals in a neighboring yard, yet they never assert that any of the individuals was holding or using a cell phone, which could indicate they were looking at online directions.[288] Regardless, an individual searching for an explosives-related term or a particular address is not in and of itself indicative of criminality.

---

[284] Affidavit in Support of an Application for a Search Warrant, *supra* note 89, ¶ 7.

[285] *Id.* ¶ 32.

[286] Motion to Suppress, *supra* note 31, ¶ 75.

[287] *Id.* ¶ 76.

[288] *Id.* ¶ 75.

a. An Internet Query is not Necessarily Indicative of Criminal Wrongdoing

In *Ybarra*, authorities obtained a search warrant for a tavern and its bartender based on an informant's tip that the bartender had packets of heroin.[289] When officers arrived to search the subjects of the warrant, they announced they would also be conducting a *Terry* frisk of the 13 patrons present.[290] The officers proceeded to pat down each of the patrons, feeling a "cigarette pack with objects in it" in the pocket of Mr. Ybarra.[291] While the cigarette pack was not removed from Mr. Ybarra's pocket during the initial pat down, he was searched again several minutes later, at which time officers discovered the pack contained heroin.[292] The Court held that at the time the warrant was issued there was "no reason to suppose that . . . the authorities had probable cause to believe that any person found on the premises of [the tavern], aside from [the bartender] would be violating the law."[293] It went on to explain a person's "mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person," and that "[t]his requirement cannot be undercut or avoided by simply pointing to the fact that coincidentally there exists probable cause to search or seize another or to search the premises where the person may happen to be."[294]

The court in *Chatrie* applied *Ybarra* to geofence warrants, holding that "a Google user's proximity to the bank robbery does not necessarily suggest that the user participated in the crime."[295] It went on to state the geofence warrant at issue provided the Government "unlimited discretion to obtain from Google the device IDs . . . of anyone whose Google-connected devices traversed the geofences (including their vaguely defined margins of error), based on nothing more than the 'propinquity' of these

---

[289] Ybarra v. Illinois, 444 U.S. 85, 87–88 (1979).

[290] *Id.* at 88.

[291] *Id.*

[292] *Id.* at 88–89.

[293] *Id.* at 90.

[294] *Id.* at 91 (citing Sibron v. New York, 392 U.S. 40, 62–63 (1968)).

[295] United States v. Chatrie, 590 F. Supp. 3d 901, 931 (E.D. Va. 2022).

persons to the Unknown Subject at or near the time" of the criminal activity.[296]

While both *Ybarra* and *Chatrie* address physical space, those swept up in the dragnet of a reverse keyword search are similarly prone to becoming patrons in the metaphorical tavern. Just like people may be within the geofence radius during its timespan for various innocuous reasons, people may search the terms sought in a reverse keyword warrant for similarly non-criminal purposes.[297]

For instance, law enforcement frequently includes addresses as a keyword in these types of warrants.[298] A person could search for an address and wind up in the warrant's dragnet if they made a typo, were house hunting, or if the same address exists in another city.[299] Similarly, investigators in the Austin serial bombing case included several terms related to pipe bombs in their keyword warrant.[300] An innocent person could search for these terms if they became curious while watching television or a movie or were writing a story about a bombing.[301]

These users–about whom law enforcement knows nothing in particular–will have their privacy invaded simply because they searched a term that authorities believe the perpetrator of a crime could have hypothetically searched.[302]

IV. CONCLUSION

The ability of people to access previously unimaginable troves of information has been rightly heralded as one of the crowning achievements of the Internet Age.[303] Considering the sheer volume of data available, search engines are critical tools that enable users to wade through the vastness and find answers to their pointed inquiries, conduct research, and

---

[296] *Id.* (quoting *In re* Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 753 (N.D. Ill. 2020)).

[297] *Id.* (citing *In re* Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730 (N.D. Ill. 2020)).

[298] Amicus Brief Supporting Defendant *supra* note 32, at 4–5.

[299] *Id.* at 11.

[300] Affidavit in Support of an Application for a Search Warrant, *supra* note 89, ¶ 2.

[301] Amicus Brief Supporting Defendant, *supra* note 32, at 4–5.

[302] *Id.* at 13; *see* Ybarra v. Illinois, 444 U.S. 85, 91 (1979).

[303] *See* Dentzel, *supra* note 1.

satisfy their curiosity.[304] None of this is possible, however, if users' freedom of inquiry is stifled by a fear of reprisal and incrimination for their queries.[305]

In his 1975 book *Discipline and Punish: The Birth of the Prison*, the French philosopher Michel Foucault discusses 19th-century social reformer Jeremy Bentham's "panopticon" prison design.[306] In a panopticon-style prison, the individual cells form a rotunda surrounding a tower from which the stationed guards can see into any cell at any time.[307] Since the prisoners would never know when they were being surveilled, Bentham theorized that they would preemptively police their own actions, assuming they were being surveilled.[308] Foucault used the panopticon as a metaphor for systems of control in modern society.[309]

One can imagine the panopticon-like impact broader awareness of reverse keyword warrants could have on users' search habits. Following whistleblower Edward Snowden's revelations about the National Security Agency (NSA)'s use of the Upstream program to intercept Internet and phone traffic, one study found a 19.5% drop in views for Wikipedia articles related to terrorism, while another found a 5% decrease in Google searches for "privacy-sensitive" terms.[310] Following the passage of the Patriot Act in October 2001, which vastly expanded the United States' surveillance apparatus, civil rights organizations and libraries raised concerns about section 215 of the act, which enabled "the FBI to ask a secret court to order production of 'any tangible things' from a third party . . . includ[ing] records, papers, documents, or books."[311] These groups were

---

[304] *See* Amicus Brief Supporting Defendant, *supra* note 32, at 17.

[305] *See id.*

[306] Thomas McMullan, *What Does the Panopticon Mean in the Age of Digital Surveillance?*, THE GUARDIAN (July 23, 2015, 3:00 PM), https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham [https://perma.cc/ATU8-NJ8V].

[307] *Id.*

[308] *Id.*

[309] *Id.*

[310] Jonathon W. Penny, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117, 131, 146 (2016).

[311] Justin Elliott, *Remember When the Patriot Act Debate Was All About Library Records?*, PROPUBLICA (June 17, 2013, 2:08 PM), https://www.propublica.org/article/remember-when-the-patriot-act-debate-was-about-library

(*continued*)

particularly concerned about the impact the FBI's monitoring and ability to demand circulation records could have on intellectual freedom.[312] The American Library Association (ALA), along with librarians around the country, spoke out against the Act calling it "a present danger to the constitutional rights and privacy rights of library users…"[313] To protect users' freedom of inquiry, the ALA adopted a resolution urging libraries to create privacy policies and to only retain records necessary to their work.[314]

Today search engines act similarly to libraries by facilitating inquiry and the flow of information.[315] Recently, Internet search giants like Google, Microsoft, and Yahoo have begun to acknowledge their distaste for reverse warrants.[316] Like libraries, they should acknowledge their role as stewards of the freedom of inquiry demands a higher duty of care with users' data.[317] If search engines changed the way they collect and retain identifiable, user-specific data so they were only in possession of the data absolutely necessary to provide their services, search engines would no

---

-records [https://perma.cc/FPJ9-E3P6].

[312] April Glaser, *Long Before Snowden, Librarians Were Anti-Surveillance Heroes*, SLATE, https://slate.com/technology/2015/06/usa-freedom-act-before-snowden-librarians-were-the-anti-surveillance-heroes.html [https://perma.cc/6XBA-MBWG] (June 4, 2015).

[313] AM. LIBR. ASS'N, RESOLUTION ON THE USA PATRIOT ACT AND RELATED MEASURES THAT INFRINGE ON THE RIGHTS OF LIBRARY USERS 2 (2003), https://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/intfreedom/statementspols/ifresolutions/usapatriotactresolution.pdf [https://perma.cc/4N9P-HHAL].

[314] *Id.*

[315] *See* Amicus Brief Supporting Defendant, *supra* note 32, at 17.

[316] *See* Guariglia, *supra* note 15 ("[T]hese warrants are so invasive of user privacy that big tech companies like Google, Microsoft, and Yahoo are willing to support banning them.").

[317] *See* Aaron Mackey & Jennifer Lynch, *It's Time for Google to Resist Geofence Warrants and to Stand Up for Its Affected Users*, EFF DEEPLINKS BLOG (Aug. 12, 2021), https://www.eff.org/deeplinks/2021/08/its-time-google-resist-geofence-warrants-and-stand-its-affected-users [https://perma.cc/MTE6-VR25] ("Google holds a tremendous amount of power over law enforcement's ability to use geofence warrants. Instead of keeping quiet about them and waiting for defendants in criminal cases to challenge them in court, Google needs to stand up for its users when it comes to revealing their sensitive data to law enforcement.").

longer be able to respond to reverse warrants, thus halting their proliferation.[318]

It is unlikely search engines will adopt these data collection and retention reforms on their own. The sale and use of the data search engines collect is their business model.[319] Advertising and data sales make up a large portion of their revenue.[320] Search engines could, however, take a page from the library profession's response to another earlier incursion on patron privacy and lobby to protect their users from government intrusion.

In 1987, the New York Times revealed that as part of the Library Awareness Program, the FBI visited libraries around the country to request that librarians "watch for and report on library users who might be diplomats of hostile powers recruiting intelligence agents or gathering information potential harmful to United States security."[321] Librarians and the ALA rallied against the Library Awareness Program and reaffirmed their commitment to patrons' privacy.[322] This led 48 states to pass or strengthen their library privacy laws.[323]

While search engines have already taken a step in the right direction by supporting legislation to ban the use of geofence and reverse keyword warrants in New York and California, they should continue to lobby for

---

[318] *Id.* ("Google must minimize its processing of user data, that is, only process user data as reasonably necessary to give users what they asked for.").

[319] Sarah Mayer, *Data Privacy Concerns with Search Engines*. CPO MAG. (Dec. 25, 2018), https://www.cpomagazine.com/data-privacy/data-privacy-concerns-with-search-engines/ [https://perma.cc/7VWN-T5WV].

[320] Felix Richter, *Google Takes Lion's Share of Search Ad Revenues*, STATISTA (Feb. 9, 2023), https://www.statista.com/chart/29271/search-advertising-market-share/ [https://perma.cc/C82L-SADF].

[321] Joan Starr, *Libraries and National Security: An Historical Review*, 9 FIRST MONDAY (2004), https://firstmonday.org/ojs/index.php/fm/article/view/1198/1118 [https://perma.cc/NY7V-BY8R].

[322] Bryan M. Carson, *Surveying Privacy: Library Privacy Laws in the Southeastern United States*, 49 SE. LIBR. 19, 19–20 (2001), https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1005&context=seln [https://perma.cc/55JB-MLQV] ("According to Vartan Gregorian, President of the New York Public Library, 'We consider reading a private act, an extension of freedom of thought. And our doors are open to all. We don't check IDs.'").

[323] *Id.* at 20; *State Privacy Laws Regarding Library Records*., AM. LIBR. ASS'N (Nov. 2021), https://www.ala.org/advocacy/privacy/statelaws [https://perma.cc/8RPQ-EZHE].

legislation outlawing these warrants in other jurisdictions and speak out against their use rather than quietly complying.[324]

As the ALA states in its interpretation of the Library Bill of Rights, "[w]hen users recognize or fear that their privacy or confidentiality is compromised, true freedom of inquiry no longer exists."[325] Until the Supreme Court or legislators act to stop the use of reverse keyword warrants, they will remain a dangerous tool in law enforcement's arsenal with a disturbing potential to erode civil liberties and chill expressive freedoms.[326]

---

[324] Riley, *supra* note 168; Mackey & Lynch, *supra* note 317.

[325] *Privacy: An Interpretation of the Library Bill of Rights*, AM. LIBR. ASS'N, https://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy [https://perma.cc/BR5Z-B3PK] (June 14, 2019).

[326] Winters, *supra* note 37, at 1393 (2023).