

**IN THE
COURT OF APPEALS OF VIRGINIA**

RECORD NO. 2032-24-4

WILLIE JAMES CLEMENTS, JR.

Appellant,

VS.

COMMONWEALTH OF VIRGINIA

Appellee.

**BRIEF OF AMICI CURIAE ELECTRONIC FRONTIER
FOUNDATION, AMERICAN CIVIL LIBERTIES UNION, AND
AMERICAN CIVIL LIBERTIES UNION OF VIRGINIA IN SUPPORT OF
APPELLANT**

**Andrew Gellis Crocker, *Pro Hac Vice* pending
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
Email: andrew@eff.org**

**Matthew William Callahan, VSB # 99823
ACLU Foundation of Virginia
PO Box 26464
Richmond, VA 23261-6464
Telephone: (804) 523-2146
Facsimile: (804) 649-2733
Email: mcallahan@acluva.org**

TABLE OF CONTENTS

	PAGE NUMBER
TABLE OF AUTHORITIES	iii
STATEMENT OF INTEREST	1
STATEMENT OF THE CASE	2
STATEMENT OF FACTS	2
STANDARD OF REVIEW	2
ASSIGNMENTS OF ERROR	2
INTRODUCTION AND SUMMARY OF ARGUMENT	3
ARGUMENT	6
I. Keyword warrants draw on vast repositories of data held by search engines, authorizing indiscriminate interference with Internet users’ privacy.	6
A. Search engines are indispensable to browsing the Internet.....	6
B. Keyword warrants enable the search of billions of users’ search queries.....	11
II. Keyword warrants harm expressive freedoms and are subject to heightened scrutiny under both the U.S. and Virginia Constitutions.....	16
A. Keyword warrants compromise expressive freedoms.	16
B. Under both the Federal and Virginia Constitutions, individuals maintain an expectation of privacy in their search queries and associated data.	20
III. The keyword warrant was an unconstitutional general warrant in violation of the Fourth Amendment and Article I, Section 10.	23
A. The Fourth Amendment and Article I, Section 10 were drafted to prohibit general warrants.....	23

B.	Keyword warrants are unconstitutional general warrants under the Fourth Amendment.....	26
C.	At a minimum, keyword warrants are unconstitutional general warrants under the Virginia Constitution.....	28
IV.	Even if it was not a general warrant, the keyword warrant in this case was insufficiently particularized and lacked probable cause to support a search of every account.	31
	CONCLUSION.....	36

TABLE OF AUTHORITIES

Cases

<i>Andresen v. Maryland</i> 427 U.S. 463 (1976)	4, 29, 40
<i>Board of Educ. v. Pico</i> 457 U.S. 853 (1982) (plurality opinion)	21, 22
<i>Byrd v. United States</i> 584 U.S. 395 (2018)	28
<i>Carpenter v. United States</i> 138 S. Ct. 2206 (2018)	passim
<i>Commonwealth v. Grossman</i> 555 A.2d 896 (Pa. 1989)	35
<i>Commonwealth v. Kurtz</i> No. 100 MAP 2023 (Pa. argued May 14, 2024) (pending)	1
<i>Commonwealth v. Santner</i> 454 A.2d 24 (Pa. Super. Ct. 1982)	25
<i>Dalia v. United States</i> 441 U.S. 238 (1979)	39
<i>Henry v. Commonwealth</i> 529 S.E.2d 796 (Va. App. 2000)	37
<i>Illinois v. Gates</i> 462 U.S. 213 (1983)	39
<i>In re Application of the U.S. for an Order Pursuant To 18 U.S.C. §2703(d)</i> No. 2:17-MC-51662, 2017 WL 6368665, (E.D. Mich. Dec. 12, 2017)	44
<i>In re Application of the U.S. for an Order Pursuant to 18 U.S.C. 2703(c), 2703(d)</i> <i>Directing AT & T, Sprint/Nextel, T-Mobile, Metro PCS, Verizon Wireless</i> 42 F. Supp. 3d 511, 519 (S.D.N.Y. 2014)	43, 44
<i>In re Google Inc. Cookie Placement Consumer Privacy Litigation</i> 806 F.3d 125, 138–39 (3d Cir. 2015)	27

<i>In re Grand Jury Subpoena to Amazon.com Dated Aug. 7, 2006</i> 246 F.R.D. 570 (W.D. Wisc. 2007)	23
<i>In re Grand Jury Subpoena to Kramerbooks & Afterwords</i> 26 Med. L. Rptr. 1599 (D.D.C. 1998).....	23
<i>In re Search of Cellular Tel. Towers</i> 945 F. Supp. 2d 769 (S.D. Tex. 2013).	45
<i>In re the Search of Information and Records Associated with Google Searches For Various Search Terms That Are Stored at Premises Controlled by Google (2), No.1:18-mj-00191-ML *SEALED* (W.D. Tex. March 2018).....</i>	17
<i>Kleindienst v. Mandel</i> 408 U.S. 753 (1972).....	21
<i>Lamont v. Postmaster Gen.</i> 381 U.S. 301 (1965).....	22, 24, 25
<i>Lowe v. Commonwealth</i> 337 S.E.2d 273 (Va. 1985).....	37
<i>Martin v. City of Struthers</i> 319 U.S. 141 (1943).....	22
<i>McClannan v. Chaplain</i> 136 Va. 1 (1923)	33
<i>McIntyre v. Ohio</i> 514 U.S. 334 (1995).....	24
<i>Payton v. New York</i> 445 U.S. 573 (1980).....	31
<i>People v. Frank</i> 700 P.2d 415 (Cal. 1985)	34
<i>People v. Seymour</i> 536 P.3d 1260 (Colo. 2023).....	1, 10, 19, 26
<i>Rakas v. Illinois</i> 439 U.S. 128, 142, 143 (1978).....	29
<i>Riley v. California</i> 573 U.S. 373 (2014).....	1, 26, 31

<i>Stanford v. Texas</i> 379 U.S. 476 (1965).....	passim
<i>Stanley v. Georgia</i> 394 U.S. 557 (1969).....	22
<i>State v. Leonard</i> 943 N.W.2d 149 (Minn. 2020).....	38
<i>State v. Wright</i> 961 N.W.2d 396 (Iowa 2021)	38
<i>Steagald v. United States</i> 451 U.S. 204 (1981).....	30
<i>Tattered Cover, Inc. v. City of Thornton</i> 44 P.3d 1044 (Colo. 2002).....	passim
<i>United States v. Bridges</i> 344 F.3d 1010 (9th Cir. 2003)	35
<i>United States v. Chatrue</i> 136 F.4th 100 (4th Cir. 2025)	12, 40, 41
<i>United States v. Cotterman</i> 709 F.3d 952, 957 (9th Cir. 2013)	26
<i>United States v. Ganius</i> 824 F.3d 199 (2d Cir. 2016)	2
<i>United States v. Hasbajrami</i> 945 F.3d 641 (2d Cir. 2019)	2
<i>United States v. Playboy Ent. Grp., Inc</i> 529 U.S. 803 (2000).....	22, 23
<i>United States v. Rumely</i> 345 U.S. 41 (1953).....	23
<i>United States v. Smith</i> 110 F.4th 817 (5th Cir. 2025)	6, 29
<i>United States v. Warshak</i> 631 F.3d 266 (6th Cir. 2010)	2, 27, 28
<i>United States v. Williams</i> 592 F.3d 511 (4th Cir. 2010).....	35

<i>United States v. Williams</i> No. 20-MJ-630 (E.D.N.Y. Aug. 4, 2020)	19
<i>Vlaming v. West Point Sch. Bd.</i> 302 Va. 504 (2023)	21, 36, 37
<i>Ybarra v. Illinois</i> 444 U.S. 85 (1979)	40
<i>Zimmerman v. Town of Bedford</i> 134 Va. 787 (1922)	5, 33
<i>Zurcher v. Stanford Daily</i> 436 U.S. 547 (1978)	5, 25
Statutes	
18 U.S.C. § 2703(c)(2)	13
Va. Code Ann. § 19.2-54 (1975)	29
Va. Code Ann. § 19.2-68(A)(3)	33
Other Authorities	
1 A.E. Dick Howard, <i>Commentaries on the Constitution of Virginia</i> 174 (1974)	23, 24, 25
<i>Access & control activity in your account</i> , Google, https://support.google.com/accounts/answer/7028918	9
Danny Sullivan, <i>How Google Autocomplete Predictions Are Generated</i> , Google (Oct. 8, 2020), https://blog.google/products/search/how-google-autocomplete-predictions-work	8
David Nield, <i>A Guide to Using Android Without Selling Your Soul to Google</i> , Gizmodo (July 26, 2018), https://gizmodo.com/a-guide-to-using-android-without-selling-your-soul-to-g-1827875582	10
Eugene Volokh, <i>Search and Seizure: Keyword Warrants</i> , Reason (Oct. 7, 2021), https://reason.com/volokh/2021/10/07/keyword-warrants/	14
Google, <i>Supplemental Information on Geofence Warrants in the United States</i> at 2 (2021), https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf (follow “Download supplemental data as a CSV” hyperlink)	11

Luke Johnson, <i>How to See EVERY Google Search You've Ever Made</i> , Digital Spy (Dec. 26, 2016), https://www.digitalspy.com/tech/a805172/how-to-see-every-google-search-youve-ever-made	10
Maryam Mohsin, <i>10 Google Search Statistics You Need to Know in 2023</i> , Oberlo (Jan. 13, 2023), https://www.oberlo.com/blog/google-search-statistics	9
Michael Arrington, <i>AOL Proudly Releases Massive Amounts of Private Data</i> , TechCrunch (Aug. 6, 2006), https://techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data	12
Naomi Gilens, et al., <i>Google Fights Dragnet Warrant for Users' Search Histories Overseas While Continuing to Give Data to Police in the U.S.</i> , EFF (Apr. 5, 2022), https://www.eff.org/deeplinks/2022/04/google-fights-dragnet-warrant-users-search-histories-overseas-while-continuing	14
<i>November 2023 Web Server Survey</i> , Netcraft (Nov 24, 2023), https://www.netcraft.com/blog/november-2023-web-server-survey/ ; <i>The Size of the World Wide Web (The Internet)</i> , Tilburg University, https://www.worldwidewebsite.com/	6
<i>Search Engine Market Share in 2023</i> , Oberlo, https://www.oberlo.com/statistics/search-engine-market-share	8
Siladitya Ray, <i>Google Shared Search Data with Feds Investigating R. Kelly Victim Intimidation Case</i> , Forbes (Oct. 8, 2020).....	15
Thomas Brewster, <i>Cops Demand Google Data on Anyone Who Searched a Person's Name... Across a Whole City</i> , Forbes (Mar. 17, 2017), https://www.forbes.com/sites/thomasbrewster/2017/03/17/google-government-data-grab-in-edina-fraud-investigation/?sh=5fe5045d7ade	11, 14
Thomas Brewster, <i>Google Dragnets Harvested Phone Data Across 13 Kenosha Protest Acts of Arson</i> , Forbes (Aug. 31, 2021).....	16
Vangie Beal, <i>Dynamic URL</i> , Webopedia (May 24, 2021), https://www.webopedia.com/TERM/D/dynamic_URL.html	7
<i>Web Crawler</i> , Wikipedia, https://en.wikipedia.org/wiki/Web_crawler ; <i>How Google Search Works</i> , Google, https://www.google.com/search/howsearchworks/how-search-works	7

WhatIsMyIP.com, https://www.whatismyip.com/ip-address-lookup	13
William J. Cuddihy, <i>The Fourth Amendment: Origins and Original Meaning</i> , 602–1791 at 363 (2009).....	23

Constitutional Provisions

U.S. Const. amend I	4, 16, 29
U.S. Const. amend IV	<i>passim</i>
Va. Const. art. I § 10	<i>passim</i>

STATEMENT OF INTEREST

The Electronic Frontier Foundation (“EFF”) is a nonprofit, member-supported digital civil liberties organization. Founded in 1990, EFF has over 30,000 active donors and dues-paying members across the United States, including in Virginia. EFF represents the interests of technology users in court cases and broader policy debates surrounding the application of law to technology. EFF regularly participates both as direct counsel and as amicus in the U.S. Supreme Court and many others in cases addressing the Fourth Amendment and its application to new technologies. *See, e.g., Carpenter v. United States*, 585 U.S. 296 (2018); *Riley v. California*, 573 U.S. 373 (2014); *People v. Seymour*, 536 P.3d 1260 (Colo. 2023) (keyword search warrant); *Commonwealth v. Kurtz*, No. 100 MAP 2023 (Pa. argued May 14, 2024) (pending) (keyword search warrant).

The American Civil Liberties Union (“ACLU”) is a nationwide, nonprofit, nonpartisan organization dedicated to the principles of liberty and equality embodied in the Constitution and our nation’s civil rights laws. The American Civil Liberties Union of Virginia (“ACLU-VA”) is the Virginia state affiliate of the national ACLU. Since its founding in 1920, the ACLU has frequently appeared before the U.S. Supreme Court and other state and federal courts in numerous cases implicating Americans’ right to privacy in the digital age, including as counsel in *Carpenter v. United States*, 585 U.S. 296 (2018), and as

amicus in *United States v. Ganius*, 824 F.3d 199 (2d Cir. 2016) (en banc), *United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019), and *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

The ACLU-VA has appeared frequently before this Court and other Virginia courts, advocating for the rights to privacy and free speech in digital media and the right to privacy generally under the Fourth Amendment to the U.S. Constitution and Article I, section 10 of the Virginia Constitution.

STATEMENT OF THE CASE

Amici concur with the Statement of the Case set forth in Appellant's opening brief.

STATEMENT OF FACTS

Amici concur with the Statement of Facts set forth in Appellant's opening brief.

STANDARD OF REVIEW

Amici concur with the Standard of Review set forth in Appellant's opening brief.

ASSIGNMENTS OF ERROR

Amici concur with the Assignments of Error set forth in Appellant's opening brief.

INTRODUCTION AND SUMMARY OF ARGUMENT

The Internet is crucial to modern life, but it is nearly impossible to navigate without using a search engine like Google. People now “Google” everything, including sensitive questions that they might never ask a human confidant. But Google—the company, not the verb—retains detailed information about search queries and the people who make them. Over the course of months and years, there is little about users’ lives that will not be reflected in their search keywords, from the mundane to the intimate. The result is a vast record, in corporate hands, of users’ most private and personal thoughts, opinions, and associations.

Of course, this trove of sensitive information can be useful to police. For example, when police have an identifiable suspect, they might seek evidence of search terms that the person has used at a relevant time—for example to see if they tried to sell illegal drugs, purchase an illegal gun, or obtain an illegal abortion. While that data, and the capability to retrieve it, is new, the approach—focused on a single, identifiable person—is not.

But “reverse searches,” like the one authorized by the keyword warrant in this case, are altogether different. Instead of seeking data concerning a single identified suspect, these searches require a company like Google to search its *entire* reserve of user data—truly, all the searches in the world—and identify users or devices that searched for words or phrases specified by police. And the sole

basis for the warrant may be an officer's hunch that someone searched for a term that is somehow indicative of criminal behavior.

Hence, keyword warrants are dragnet searches. Like eighteenth-century writs of assistance that motivated the drafters of the Fourth Amendment to the U.S. Constitution and Article I, Section 10 of the Virginia Constitution, keyword warrants are general warrants that authorize "a general, exploratory rummaging in a person's belongings." *Andresen v. Maryland*, 427 U.S. 463 (1976). They are therefore prohibited by both the Fourth Amendment and Article I, Section 10. *Id.*; *Zimmerman v. Town of Bedford*, 134 Va. 787, 800–02, 115 S.E. 362 (1922). And like those writs, keyword warrants are especially pernicious because, beyond sweeping up countless innocent individuals, they target protected speech and the corollary right to receive information. *See Stanford v. Texas*, 379 U.S. 476, 482–83 (1965); *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1051–52 (Colo. 2002) (en banc), *as modified on denial of reh'g* (Apr. 29, 2002); *Zurcher v. Stanford Daily*, 436 U.S. 547, 564, 565 (1978) (search impacting First Amendment interests subject to heightened scrutiny).

The Commonwealth will likely argue that the warrant in this case was sufficiently narrow because it retrieved only data concerning Internet searches within a defined time period and of a particular address. But that argument runs afoul of the U.S. Supreme Court's reasoning in *Carpenter v. United States*, 585

U.S. 296, 311–12 (2018). In *Carpenter*, investigators acquired two days’ worth of an identified suspect’s cell site location information (“CSLI”) generated by his cell phone. *Id.* at 310 n.3. But, to assess whether the suspect had a constitutionally protected privacy interest in the CSLI, the Supreme Court looked beyond the specific results of the search in that case and instead focused on the general capability of CSLI searches “to chronicle a person’s past movements.” *Id.* at 309. Here, the trial court correctly determined that there is a reasonable expectation of privacy in search queries, noting that a categorical rule was preferable to analyzing specific search terms to determine which were private. R. 497 (Order on Mot. to Suppress at 9-10). And although the court rejected the argument that the keyword warrant was an unconstitutional general warrant, it correctly appreciated that *Carpenter*’s discussion of capability not only informs the question of expectation of privacy, but of whether a technique constitutes a general search. *Id.* See also *United States v. Smith*, 110 F.4th 817, 824–25 (5th Cir. 2025) (geofence warrants, another type of reverse search, are categorically unconstitutional).

Because the warrant in this case purported to authorize a search that can reveal the intimate matters of vast numbers of people, targets speech, lacks probable cause, and is overbroad, it is an impermissible general warrant.

ARGUMENT

I. Keyword warrants draw on vast repositories of data held by search engines, authorizing indiscriminate interference with Internet users' privacy.

A. Search engines are indispensable to browsing the Internet.

Keyword warrants are valuable to the police only because it is virtually impossible to locate information on the Internet without entering search terms (also known as “keywords”) into a search engine. According to some sources, there are about 1.1 billion websites and tens of billions of webpages.¹ Similar to street addresses in the physical world, each webpage has a unique address -- called a URL (“uniform resource locator”) -- in the online world. The URL serves as both a location and as directions for a user’s browser to find and display a particular webpage. URLs can contain the website’s domain name, such as “Google.com,” as well as additional information that may be much more complex. For example, the domain for the Virginia courts website is vacourts.gov, and the specific URL for instructions on filing a brief in this Court is <https://www.vacourts.gov/static/online/vjefs/usersmanual.pdf>. URLs can be quite long and are often “dynamic,”

¹ *November 2023 Web Server Survey*, Netcraft (Nov 24, 2023), <https://www.netcraft.com/blog/november-2023-web-server-survey/>; *The Size of the World Wide Web (The Internet)*, Tilburg University, <https://www.worldwidewebsize.com/>.

meaning they change based on users' search queries, among other circumstances.²

Search engines are therefore often the only practical way to find a particular webpage. For example, if someone wanted to get directions to this Court using Google Maps, but without using a Google search, they would need to type:

https://www.google.com/maps/place/100+N+9th+St+5th+Floor,+Richmond,+VA+23219/@37.5396083,-77.4382979,17z/data=!3m1!4b1!4m5!3m4!1s0x89b11122cb2326c9:0x7156003786c206b3!8m2!3d37.5396083!4d-77.4357176?entry=ttu&g_ep=EgoyMDI1MDUyOC4wIKXMDSOASAFQAw%3D%3D —or just use a search engine.

Search engines also make it possible to find specific content within websites, including text, video, images, and documents. Search engines continuously scour the Internet for content, index and organize the information they find into vast databases, and rank that information based on its relevance to search queries.³ And, of course, the more detailed the keywords that people type into search engines, the more likely they are to find exactly the content they are seeking.

² Vangie Beal, *Dynamic URL*, Webopedia (May 24, 2021), https://www.webopedia.com/TERM/D/dynamic_URL.html.

³ *Web Crawler*, Wikipedia, https://en.wikipedia.org/wiki/Web_crawler; *How Google Search Works*, Google, <https://www.google.com/search/howsearchworks/how-search-works>.

In consequence, reverse keyword searches can be incredibly revealing. Internet users frequently search for answers to medical questions, information about controversial ideas, and discussions of gender and sexuality, to give just a few examples. And there are plenty of legitimate reasons people might search for seemingly more “incriminating” information. A crime novelist could search for unique ways to kill people, a historian of the civil rights era could search for racist language, and a prosecutor or criminal defense lawyer might search for specifics on how drugs are manufactured and used.

At the same time, reverse keyword searches can also yield misleading or overinclusive results. For example, modern search engines offer an “autocomplete” feature, which relies on sophisticated algorithms to make predictions about what the user might be seeking.⁴ If someone accidentally clicks on one of these predictions, or if they click intentionally based on a whim, the keywords in the resulting search might tend to suggest facts about them that are not really true.

Google Search is far and away the most popular search engine, with nearly 92% worldwide market share (89% in the United States),⁵ and “more than 1 billion

⁴ Danny Sullivan, *How Google Autocomplete Predictions Are Generated*, Google (Oct. 8, 2020), <https://blog.google/products/search/how-google-autocomplete-predictions-work>.

⁵ *Search Engine Market Share in 2023*, Oberlo, <https://www.oberlo.com/statistics/search-engine-market-share>.

average monthly users.”⁶ Most people use Google to search the Internet at least three times per day,⁷ yielding a total of over 8.5 billion searches per day.⁸ As of 2019, 63% of those searches were conducted on mobile devices.⁹

Due to its market dominance, Google possesses massive amounts of information about users’ searches. For users logged into their accounts, Google keeps a record of all search queries and stores that data along with other information about the user, including what videos they have watched, what images they have viewed, what websites they have visited, where they have traveled, and who they are.¹⁰ Google now allows users to delete search history and to turn off Google’s collection of that data.¹¹ However, if users do not take active steps to delete their data, Google will likely have a record of everything they have ever

⁶ See *Seymour*, 536 P.3d at 1260 (Seymour C.A.R. 21 Petition, Exh. 4, Decl. of Nikki Adeli ¶ 4), available at <https://www.eff.org/document/people-v-seymour-google-declaration-colorado-keyword-search> (hereinafter “Google Decl.”).

⁷ Maryam Mohsin, *10 Google Search Statistics You Need to Know in 2023*, Oberlo (Jan. 13, 2023), <https://www.oberlo.com/blog/google-search-statistics>.

⁸ *Id.*

⁹ *Id.*

¹⁰ See *Access & control activity in your account*, Google, <https://support.google.com/accounts/answer/7028918>.

¹¹ *Id.*; Google Decl. ¶ 5.

searched for, dating back years.¹² *See also United States v. Chatrue*, 136 F.4th 100, 127–29 (4th Cir. 2025) (en banc) (Wynn, J., concurring) (discussing the difficulty of deleting location history from Google user account).

Google retains data on *everyone* who uses its search engine, not just Google users who are logged into their accounts. Google links every search to a device’s IP address. With that information, an officer can easily connect a search to a specific person.¹³ That makes it very difficult to search Google anonymously, whether via a personal computer or a handheld device.¹⁴ It is unclear how long Google retains search history data from people who are not logged into Google accounts, but for logged-in users Google’s database goes back at least 18 months.¹⁵

¹² Luke Johnson, *How to See EVERY Google Search You’ve Ever Made*, Digital Spy (Dec. 26, 2016), <https://www.digitalspy.com/tech/a805172/how-to-see-every-google-search-youve-ever-made>.

¹³ *See, e.g.*, Google Decl. ¶¶ 5–9.

¹⁴ For Android device users, it is particularly difficult to search without being logged into a Google account. David Nield, *A Guide to Using Android Without Selling Your Soul to Google*, Gizmodo (July 26, 2018), <https://gizmodo.com/a-guide-to-using-android-without-selling-your-soul-to-g-1827875582>.

¹⁵ Alex Hern, *Google says it will no longer save a complete record of every search*, The Guardian (June 24, 2020), <https://www.theguardian.com/technology/2020/jun/24/google-says-it-will-no-longer-save-a-complete-record-of-every-search>

B. Keyword warrants enable the search of billions of users’ search queries.

Keyword search warrants are relatively new—they were first reported in the press in 2017¹⁶ -- and it is unclear how many are issued each year. But if they are anything like another novel dragnet method used to identify suspects -- “geofence warrants”¹⁷ -- their use is likely increasing. Geofence warrants now make up 25% of all warrants Google receives, and in Virginia the number of geofence warrants recently increased six-fold, from 74 in 2018 to 484 in 2020.¹⁸

But keyword search warrants, which have no geographic limits, sweep even more broadly than geofence warrants, which do. Google has stated it must search its entire database of users’ search queries within the relevant time period to comply with a keyword warrant, including users with no connection to the area of the alleged crime.¹⁹ This is because the warrant does not identify a particular

¹⁶ Thomas Brewster, *Cops Demand Google Data on Anyone Who Searched a Person’s Name... Across a Whole City*, Forbes (Mar. 17, 2017), <https://www.forbes.com/sites/thomasbrewster/2017/03/17/google-government-data-grab-in-edina-fraud-investigation/?sh=5fe5045d7ade>.

¹⁷ Geofence warrants seek information on every device that might have been within designated geographic areas and time periods in the past.

¹⁸ Google, *Supplemental Information on Geofence Warrants in the United States* at 2 (2021), https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf (follow “Download supplemental data as a CSV” hyperlink).

¹⁹ See Google Decl. ¶ 4.

account or device but instead seeks *any* device that may have searched for the specified terms during the relevant time period.

Once police have this information, they can discover the most sensitive matters about these Google users. They can even identify people who are unfortunately caught in the net. Even seemingly impersonal and innocuous queries can reveal someone's identity. In 2006, AOL published three months of de-identified search history data from 650,000 users.²⁰ With that data, the *New York Times* was easily able to identify "Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga., frequently researches her friends' medical ailments and loves her three dogs."²¹ Studies continue to show how easy it is to identify people from their pseudonymized web browsing histories.²²

²⁰ Michael Arrington, *AOL Proudly Releases Massive Amounts of Private Data*, TechCrunch (Aug. 6, 2006), <https://techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data>.

²¹ Michael Barbaro & Tom Zeller Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. Times (Aug. 9, 2006), <https://www.nytimes.com/2006/08/09/technology/09aol.html>.

²² Lukasz Olejnik, Claude Castelluccia, & Artur Janc, *Why Johnny Can't Browse in Peace: On the Uniqueness of Web Browsing History Patterns*, 5th Workshop on Hot Topics in Privacy Enhancing Technologies (Jul 2012), Jessica Su et al., *De-anonymizing Web Browsing Data with Social Networks*, WWW '17: Procs. of the 26th Int'l Conf. on World Wide Web 1261 (Apr. 2017), available at <https://www.cs.princeton.edu/~arvindn/publications/browsing-history-deanonimization.pdf>; Sarah Bird, Ilana Segall, & Martin Lopatka, *Replication: Why We Still Can't Browse in Peace: On the Uniqueness and Reidentifiability of Web Browsing*

In response to a keyword warrant, Google may not immediately turn over the names of users who searched for specific keywords.²³ However, some publicly reported warrants have been used to obtain IP addresses, account information, and “User Agent Strings,” web browsing tracking information called “cookies,” or similar information that can reveal identity.²⁴ Once police know an IP address they do not need Google to determine who entered the search query. They may determine the ISP associated with an IP address using a simple lookup tool.²⁵ At that point, police can submit a simple subpoena to the ISP for billing records—including name and address—associated with that IP address.²⁶

Because keyword warrants require Google to search its entire data repository, they can implicate innocent people who happen to search for something potentially incriminating. While there are not many public examples of keyword warrants, the ones we know about can be quite broad. In response to a series of bombings in Austin, Texas, police sought to identify everyone who searched for

Histories, USENIX Ass’n: 16th Symp. on Usable Privacy & Sec. (Aug. 2020), available at <https://www.usenix.org/system/files/soups2020-bird.pdf> (finding 99% of browsing histories are unique).

²³ Google Decl. ¶¶ 7–9 (describing process).

²⁴ *Id.* ¶ 7.

²⁵ *See, e.g.*, WhatIsMyIP.com, <https://www.whatismyip.com/ip-address-lookup>.

²⁶ *See* 18 U.S.C. § 2703(c)(2).

words like “low explosives” and “pipe bomb.”²⁷ And in Brazil, prosecutors sought a warrant for information about everyone who searched for the name of a popular politician who was assassinated and the busy street in Rio de Janeiro where she was killed.²⁸ Even keyword search warrants that appear to be facially narrow can sweep in innocent people because of the prevalence and volume of search queries. Keyword search warrants have also been sought and issued for variations of a fraud victim’s name over a period of five weeks.²⁹ And federal law enforcement obtained information on anyone who had searched for an abducted minor’s name and address over 16 days across the year. The record does not reveal which data Google sent to the government, nor how many users were included.³⁰ Of course, anyone who knew about these incidents might have searched the victims’ names to look for news about the investigation, hoping for resolution such as the minor’s

²⁷ Affidavit ¶ 2, *In re the Search of Information and Records Associated with Google Searches For Various Search Terms That Are Stored at Premises Controlled by Google (2)*, No.1:18-mj-00191-ML *SEALED* (W.D. Tex. March 2018), available at <https://www.documentcloud.org/documents/21077351-google-keyword-warrant-in-austin-2018/>.

²⁸ Naomi Gilens, et al., *Google Fights Dragnet Warrant for Users’ Search Histories Overseas While Continuing to Give Data to Police in the U.S.*, EFF (Apr. 5, 2022), <https://www.eff.org/deeplinks/2022/04/google-fights-dragnet-warrant-users-search-histories-overseas-while-continuing>.

²⁹ Brewster, *supra* note 16.

³⁰ Eugene Volokh, *Search and Seizure: Keyword Warrants*, Reason (Oct. 7, 2021), <https://reason.com/volokh/2021/10/07/keyword-warrants/>.

safe return. So too for anyone who searched for information about these names, no matter how common, for other non-criminal reasons. Once any of these innocent users was caught in the net, police could seek a warrant for each user’s full search history, potentially revealing personal and innocent information forever.

Several known keyword warrants have, as in this case, sought to identify everyone who searched for a specific address.³¹ Yet, even a simple query for an address can be highly revealing. For example, knowing that a person searched for “201 N. Hamilton Street,” the address of a Planned Parenthood location in Richmond, could lead to an inference that the person was seeking sensitive health care.

Given the vast amount of sensitive information Google holds, keyword warrants could also allow officers to target people based on political speech or their association with others. Police used multiple geofence warrants to identify people at political protests in Kenosha, Wisconsin, and Minneapolis after police

³¹ See, e.g., Siladitya Ray, *Google Shared Search Data with Feds Investigating R. Kelly Victim Intimidation Case*, Forbes (Oct. 8, 2020), <https://www.forbes.com/sites/siladityaray/2020/10/08/google-shared-search-data-with-feds-investigating-r-kelly-victim-intimidation-case/?sh=7a4a7b847c62>; *United States v. Williams*, No. 20-MJ-630 (E.D.N.Y. Aug. 4, 2020), available at <https://www.courthousenews.com/wp-content/uploads/2020/08/Michael-Williams-Complaint.pdf>; see also *People v. Seymour*, 536 P.3d 1260 (Colo. 2023) (keyword warrant constitutionally defective, but evidence admitted under good-faith exception).

killings in those cities.³² Keyword warrants could be used the same way: officers could seek to identify everyone who searched for the address or the organizers of a protest.

II. Keyword warrants harm expressive freedoms and are subject to heightened scrutiny under both the U.S. and Virginia Constitutions.

Keyword warrants target expressive activity, including the queries entered by Internet users and the information they receive in response to those queries. Keyword warrants therefore compromise expressive freedoms guaranteed by the First Amendment and Article I, Section 12 of the Virginia Constitution.³³

A. Keyword warrants compromise expressive freedoms.

The U.S. Supreme Court has held repeatedly that the right to receive information is a “corollary of the rights of free speech and press” belonging to both speakers and their audience. *Board of Educ. v. Pico*, 457 U.S. 853, 867 (1982) (plurality opinion); *see also Kleindienst v. Mandel*, 408 U.S. 753, 762–763 (1972) (cataloging right to receive information in a “variety of contexts”); *Martin v. City*

³² Thomas Brewster, *Google Dragnets Harvested Phone Data Across 13 Kenosha Protest Acts of Arson*, Forbes (Aug. 31, 2021), <https://www.forbes.com/sites/thomasbrewster/2021/08/31/google-drag-nets-on-phone-data-across-13-kenosha-protest-arsons>; Zack Whittaker, *Minneapolis Police Tapped Google to Identify George Floyd Protesters*, TechCrunch (Feb. 6, 2021), <https://techcrunch.com/2021/02/06/minneapolis-protests-geofence-warrant>.

³³ *See Vlaming v. West Point Sch. Bd.*, 302 Va. 504, 564 (2023) (noting that the free speech protections under Article I, Section 12 are “at least as strong as” the protections under the First Amendment).

of *Struthers*, 319 U.S. 141, 146–47 (1943). A speaker’s exercise of the freedom to disseminate information would be futile if others were prohibited from receiving it. “It would be a barren marketplace of ideas that had only sellers and no buyers.” *Pico*, 457 U.S. at 867 (quoting *Lamont v. Postmaster Gen.*, 381 U.S. 301, 308 (1965) (Brennan, J., concurring)).

The right to receive information is also “a necessary predicate to the recipient’s meaningful exercise of his own rights of speech, press, and political freedom.” *Pico*, 457 U.S. at 867. It is through listening to others’ speech that “our personalities are formed and expressed” and “our convictions and beliefs are influenced, expressed, and tested” so that we can “bring those beliefs to bear on Government and on society.” *United States v. Playboy Ent. Grp., Inc.*, 529 U.S. 803, 817 (2000). Hence, “[t]he citizen is entitled to seek out or reject certain ideas or influences without Government interference or control.” *Id.*; *Stanley v. Georgia*, 394 U.S. 557, 565 (1969).

As a result, the U.S. Supreme Court and other courts have expressed United States v. Rumely, 345 U.S. 41, 57 (1953) United States v. Rumely, 345 U.S. 41, 57 (1953) special concern over government attempts to discover people’s interest in specific reading material. See *Playboy Ent. Grp., Inc.*, 529 U.S. at 817; *United States v. Rumely*, 345 U.S. 41, 57 (1953) (Douglas, J., concurring) (“Once the government can demand of a publisher the names of the purchasers of his

publications [f]ear of criticism goes with every person into the bookstall.”).

For example, in *Tattered Cover*, the Supreme Court of Colorado required a heightened showing and adversarial hearing in addition to the ordinary warrant requirements before enforcing a warrant to a bookstore for customer purchase records. 44 P.3d at 1051. And federal district courts have subjected subpoenas for customer reading lists to heightened scrutiny. *In re Grand Jury Subpoena to Kramerbooks & Afterwords*, 26 Med. L. Rptr. 1599, 1601 (D.D.C. 1998) (heightened showing required for subpoena for individual customer’s book purchases); *In re Grand Jury Subpoena to Amazon.com Dated Aug. 7, 2006*, 246 F.R.D. 570, 571–73 (W.D. Wisc. 2007) (quashing subpoena for identities of 120 book buyers) (“[I]t is an unsettling and un-American scenario to envision federal agents nosing through the reading lists of law-abiding citizens while hunting for evidence against somebody else.”). Searches of places such as bookstores and libraries, which allow people to access reading material, are especially disfavored. As the Colorado Supreme Court held in *Tattered Cover*, readers are entitled to anonymity in requesting information “because of the chilling effects that can result from disclosure of identity.” 44 P.3d at 1052 (citing *McIntyre v. Ohio*, 514 U.S. 334, 357 (1995); *Lamont*, 381 U.S. at 307 (striking down a federal statute that required citizens who wished to receive “communist political propaganda” to affirmatively notify the post office).

Investigations of online search queries resemble investigations seeking records held by physical bookstores and libraries. Like bookstores, search engines are “places where a citizen can explore ideas, receive information, and discover myriad perspectives on every topic imaginable.” *Tattered Cover*, 44 P.3d at 1052. And as with reading lists, disclosure of users’ search queries chills their right to seek out information and deters participation in the “uninhibited, robust, and wide-open debate and discussion” contemplated by the Constitution. *Lamont*, 381 U.S. at 307; *see also Tattered Cover*, 44 P.3d at 1050 (detailing evidence that search warrant for bookstore’s patron list deterred customers’ willingness to purchase “controversial books”).

When a government search directly implicates expressive activity, the U.S. Supreme Court has correspondingly required that the Fourth Amendment “preconditions for a warrant—probable cause, specificity with respect to the place to be searched and the things to be seized, and overall reasonableness”—be applied with “scrupulous exactitude.” *Zurcher*, 436 U.S. at 565, 564 (quoting *Stanford*, 379 U.S. at 485); *see also Commonwealth v. Santner*, 454 A.2d 24, 31 (Pa. Super. Ct. 1982) (citing *Stanford* and suppressing warrant that resulted in seizure of medical records reflecting what “patients had told their doctor”). Because Article I, Section 10 of the Virginia Constitution provides at least as much protection as the Fourth

Amendment, *see infra* Part III.B, the same exactitude must be used when analyzing the state constitution as well.

B. Under both the Federal and Virginia Constitutions, individuals maintain an expectation of privacy in their search queries and associated data.

U.S. Supreme Court precedent establishes that users maintain an expectation of privacy in sensitive digital communications like their Internet search queries. Such communications are protected as the modern equivalent of “papers and effects” enshrined in the Fourth Amendment. *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013) (en banc) (“The papers we create and maintain not only in physical but also in digital form reflect our most private thoughts and activities.”). Like the location data in *Carpenter* that the U.S. Supreme Court held is protected by the Fourth Amendment, “an individual’s Google search history ‘hold[s] for many Americans the privacies of life.’” *Seymour*, 536 P.3d at 1271 (quoting *Carpenter*, 585 U.S. at 311); *Riley*, 573 U.S. at 395 (“An Internet search and browsing history. . . could reveal an individual’s private interests or concerns.”)

Because of the sensitive and private information contained in our digital communications, courts have recognized they are entitled to constitutional protection even though they are transmitted by and stored with third parties like Google. *See United States v. Warshak*, 631 F.3d 266, 285–86 (6th Cir. 2010)

(Fourth Amendment protects email stored by third party).³⁴ Courts have also identified certain business records—like the customer book purchase records discussed above—that are maintained by third parties but are nevertheless constitutionally protected due to their potentially sensitive nature and the chilling effects that could result from their disclosure. *See, e.g., Carpenter*, 585 U.S. at 309–10; *Tattered Cover*, 44 P.3d at 1051. Search queries are analogous to these other communications. *See, e.g., In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125, 138–39 (3d Cir. 2015) (search queries as “content” of communications).

Finally, Google’s terms of service (TOS) cannot undercut users’ expectations of privacy. Like the email provider in *Warshak*, 631 F.3d at 286, Google and every other major commercial service provider inform their users that the service reserves the right to access user information and disclose information to law enforcement to protect the business’s interests, rights, and property.

³⁴ Since *Warshak*, courts have routinely held that individuals have a reasonable expectation of privacy in their email held in accounts operated by third party providers. Every U.S. Supreme Court justice in *Carpenter* has agreed, at least in dicta. *See* 585 U.S. at 319 (majority op., Roberts, C. J., joined by Ginsberg, Breyer, Sotomayor, and Kagan, JJ.) (noting that contents of communications are protected.); *id.* at 332 (Kennedy, J., dissenting, joined by Thomas and Alito, JJ.) (agreeing that contents of communications are protected); *id.* at 387, 400 (Gorsuch, J., dissenting) (agreeing that contents of communications are protected).

Nevertheless, in *Warshak* the Sixth Circuit concluded that this reservation of rights did not defeat an individual's reasonable expectation of privacy in email. *Id.*

The U.S. Supreme Court has also rejected the argument that private form contracts can limit or nullify a person's Fourth Amendment rights vis-à-vis the government. *See Byrd v. United States*, 584 U.S. 395 (2018). In *Byrd*, the Court held that drivers can have a reasonable expectation of privacy in a rental car even when they are driving the car in violation of the rental agreement. *Id.* at 407–08, 411. Like terms of service, these agreements “concern risk allocation between private parties. . . . But that risk allocation has little to do with whether one would have a reasonable expectation of privacy in the rental car if, for example, he or she otherwise has lawful possession of and control over the car.” *Id.*³⁵

Indeed, because all service providers impose TOS similar to Google's, holding that those terms of service can extinguish constitutional rights would arguably jeopardize constitutional rights in all kinds of data stored with third parties, potentially including texts, emails, photos, videos, and documents. Such a holding

³⁵ *See also Rakas v. Illinois*, 439 U.S. 128, 142, 143 (1978) (“arcane distinctions developed in property and tort law . . . ought not to control” the analysis of who has a “legally sufficient interest in a place”); *Smith v. Maryland*, 442 U.S. 735, 745 (1979) (“We are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation.”).

could therefore risk privacy protections for the hundreds of millions of people who use these services.

III. The keyword warrant was an unconstitutional general warrant in violation of the Fourth Amendment and Article I, Section 10.

Beyond implicating expressive freedoms, keyword searches involve the kind of indiscriminate government searches that animated the adoption of the Fourth Amendment and the textually stronger protections in Article I, Section 10 of the Virginia Constitution. As explained below, keyword warrants constitute “general warrants,” in violation of both the Fourth Amendment and Article I, Section 10.

A. The Fourth Amendment and Article I, Section 10 were drafted to prohibit general warrants.

“Since at least the mid-eighteenth century, protections against arbitrary searches and seizures have been ‘permanent monuments’ of Anglo-American law.”¹ A.E. Dick Howard, *Commentaries on the Constitution of Virginia* 174 (1974). In the American colonies, British agents used general warrants, including “writs of assistance,” to conduct broad searches for smuggled goods, limited only by the agents’ own discretion. *See Stanford*, 379 U.S. at 481–82.³⁶ “The general warrant specified only an offense . . . and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be

³⁶ See also William J. Cuddihy, *The Fourth Amendment: Origins and Original Meaning*, 602–1791 at 363 (2009).

searched.” *Steagald v. United States*, 451 U.S. 204, 220 (1981). “Opposition to such searches was in fact one of the driving forces behind the Revolution itself.” *Riley*, 573 U.S. at 403; *see also* Howard, *supra*, at 175–77.

General warrants had particularly pernicious effects on the exercise of expressive freedoms. Discussing the British “use of general warrants as instruments of oppression,” the U.S. Supreme Court commented that “this history is largely a history of conflict between the Crown and the press.” *Stanford*, 379 U.S. at 482. In particular, two British cases of the 1760s, *Wilkes v. Wood* and *Entick v. Carrington*, both centered on general warrants intended to suppress allegedly libelous publications. *Id.* at 483. “The Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression.” *Id.* at 484; *Payton v. New York*, 445 U.S. 573, 608 (1980) (White, J., dissenting) (“[D]ecisions granting recovery to parties arrested or searched under general warrants on suspicion of seditious libel” were “fresh in the colonists’ minds”).

Article I, Section 10 of the Virginia Constitution was likewise drafted in response to the “detested” practice of general warrants. Howard, *supra*, at 176. At the time, the Crown regularly issued general warrants to enforce the Navigation Acts and tax colonial trade. *Id.* at 176. The drafters of the Virginia Constitution sought to

protect Virginians from such oppressive measures used by the British in both England and the colonies. *Id.* at 175–76.

Virginians were particularly influenced by the arguments of James Otis in the famous *Paxton’s Case* challenging general warrants and writs of assistance. Howard, *supra*, at 176–77. Otis described general warrants as “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 law book.” *Boyd v. United States*, 116 U.S. 616, 625 (1886) (citation omitted). “[T]he impression that Otis” “made on colonial thinkers,” including Virginians, “was profound and was to bear fruit in the constitutions that they drafted.” Howard *supra*, at 177.

In Virginia, colonists responded to “oppressive” general warrants with Article I, Section 10 of the Virginia Constitution, which provides “[t]hat general warrants, whereby an officer or messenger may be commanded to search suspected places without evidence of a fact committed, or to seize any person or persons not named, or whose offense is not particularly described and supported by evidence, are grievous and oppressive, and ought not to be granted.” This strong language -- arguably the strongest prohibition against general warrants in the nation -- demonstrates the severity of eighteenth-century Virginians’ opposition to general warrants.

Thus, in banning general warrants, both the Fourth Amendment and Article I, Section 10, sought to prohibit exploratory rummaging into individuals' protected expression. *Stanford*, 379 U.S. at 481 (Fourth Amendment “reflect[s] the determination of those who wrote the Bill of Rights that the people of this new Nation should forever ‘be secure in their persons, houses, papers, and effects’ from intrusion and seizure by officers acting under the unbridled authority of a general warrant”); *McClannan v. Chaplain*, 136 Va. 1, 14 -16 (1923); *Zimmerman v. Town of Bedford*, 134 Va. 787, 800–02 (1922).

B. Keyword warrants are unconstitutional general warrants under the Fourth Amendment.

A warrant purporting to authorize a reverse keyword search is a digital equivalent to a warrant that purports to authorize officers to search every house in an area of a town -- simply on the chance that they might find written material connected to a crime. Like the general warrants and writs of assistance used in England and colonial America, a keyword warrant's lack of particularity and overbreadth “invite[] the police to treat [the authorization] merely as an excuse to conduct an unconstitutional general search.” *People v. Frank*, 700 P.2d 415, 422 (Cal. 1985). The kind of search a keyword warrant envisions was not conceivable, much less possible, at the nation's founding. Retrospective search query data held by Google “gives police access to a category of information otherwise

unknowable.” *Carpenter*, 585 U.S. at 312. Like cell site location information, it allows the police to “travel back in time” to reconstruct a person’s queries. *Id.* And this data is even more sensitive than CSLI because it reveals the innermost thoughts of the public.

Keyword warrants do not target particular suspects or even particular accounts. Instead, based on a hypothesis that an unknown perpetrator searched for something incriminating, they seek information on *all* accounts associated with devices that might have searched for the listed words or phrases. To comply, Google must essentially go, like the reviled constables of old, “door to door,” trawling through *all* of its users’ search data—*hundreds of millions* of user accounts—just to extract the subset of information responsive to the warrant.³⁷

With a proper search warrant, nothing is left to the discretion of the officer executing the search. *United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010). (“The particularity requirement is fulfilled when the warrant identifies the items to be seized by their relation to designated crimes and when the description of the items leaves nothing to the discretion of the officer executing the warrant.”). But when a warrant’s language is broad or ambiguous, it is more likely to reach information for which there is no probable cause. *Id.* Similarly, where the categories of records

³⁷ Google Decl. ¶ 4.

sought are so sweeping as to include anyone who searched for a phrase, there is an “unreasonable discrepancy between the items for which there was probable cause and the description in the warrant.” *Commonwealth v. Grossman*, 555 A.2d 896, 900 (Pa. 1989). As the Ninth Circuit has explained, search warrants that are “so bountiful and expansive in their language that they constitute a virtual, all-encompassing dragnet” of information “to be seized at the discretion of the State” are “fundamentally offensive to the underlying principles of the Fourth Amendment.” *United States v. Bridges*, 344 F.3d 1010, 1016 (9th Cir. 2003).

Keyword warrants compel Google to release data to the police that may include search history for people with no connection to the crime under investigation. This kind of search turns every user into a suspect and is prohibited by the Fourth Amendment.

C. At a minimum, keyword warrants are unconstitutional general warrants under the Virginia Constitution.

Regardless of whether they are deemed to be unconstitutional general warrants under the Fourth Amendment, keyword warrants violate the separate prohibition against general warrants in Article I, Section 10 of the Virginia Constitution. This Court is “absolutely free to interpret state constitutional provisions to accord greater protection than federal-court interpretations of similar

provisions of the United States Constitution.” *Vlaming v. W. Point Sch. Bd.*, 895 S.E.2d 705, 716 (Va. 2023) (cleaned up). It should do so here.

Most important, Virginia’s constitutional text is broader than its federal analog, and it arguably contains the country’s strongest prohibition against general warrants. This language of Article I, Section 10 goes far beyond the federal Constitution and demonstrates particular opposition to general warrants, as evidenced by the views of eighteenth-century Virginians, *see supra* Part III.A, and as memorialized in statute by twentieth-century Virginians, *see* Va. Code Ann. § 19.2-54 (1975) (“[N]o general warrant for the search of a house, place, compartment, vehicle or baggage shall be issued”).

In cases not implicating the ban on general warrants, Virginia courts have interpreted Section 10 coextensively with the Fourth Amendment. *See, e.g., Lowe v. Commonwealth*, 337 S.E.2d 273, 274 & n.1 (Va. 1985); *Henry v. Commonwealth*, 529 S.E.2d 796, 798 (Va. App. 2000) (collecting cases). But the reasoning of those cases does not extend to Section 10’s text concerning general warrants, because that text simply has no analogous language in the U.S. Constitution to be coextensive with. *Cf. Vlaming*, 302 Va. at 529–30 (discussing “the marked textual differences between the religion clauses of the First Amendment of the United States Constitution and the free-exercise provisions of the Constitution of Virginia”).

In any event, there is good reason for courts to consider search and seizure protections with a fresh eye. As the Iowa Supreme Court recently acknowledged, “Fourth Amendment jurisprudence is in flux,” and “[t]here are competing, inconsistent doctrines governing seizure and search law.” *State v. Wright*, 961 N.W.2d 396, 411 (Iowa 2021). This is particularly true with respect to reverse searches, where “the absence of controlling Fourth Amendment precedent” leaves ample room for this Court to interpret the Virginia Constitution in a manner robustly protecting Virginians’ rights. *See State v. Leonard*, 943 N.W.2d 149, 155–56 & n.9 (Minn. 2020). Thus, “[g]iven the uncertainty and lack of clarity in federal search and seizure jurisprudence,” as well as Virginia’s express constitutional language prohibiting general warrants, in this case there is no need “to follow federal precedents in lockstep.” *Wright*, 961 N.W.2d at 411–12.

As explained above, keyword search warrants allow officers broad discretion to search hundreds of thousands, if not millions, of unnamed and unspecified individuals—without probable cause, much less any specific evidence that any of them actually committed a crime. They are therefore general warrants that, under the Virginia Constitution, are “grievous and oppressive, and ought not to be granted.” Va. Const. art. I, § 10.

IV. Even if it was not a general warrant, the keyword warrant in this case was insufficiently particularized and lacked probable cause to support a search of every account.

Even if keyword warrants are not categorically unconstitutional general warrants, they must satisfy the requirements of particularity and probable cause on a case-by-case basis. *See Dalia v. United States*, 441 U.S. 238, 255 (1979). The keyword warrant in this case failed to do so.

First, the warrant in this case was based on the affiant's speculation that the perpetrator may have searched for the victim's house. The only connection to Google for this hunch was that its search engine is dominant, suggesting that if the perpetrator had conducted such a query, Google would have a record of it. An affidavit "must provide the magistrate with a *substantial* basis for determining the existence of probable cause." *Illinois v. Gates*, 462 U.S. 213, 239 (1983) (emphasis added). The affidavit in this case failed to do so.

Second, even if the trial court were correct that the affidavit demonstrated a probable cause that the warrant would uncover the identity of the individual perpetrator, R. 498 (Order on Mot. to Dismiss at 10), this is insufficient to provide probable cause to support a search of an unknown number of users and their search queries. Under both the Fourth Amendment and Article I, Section 10, warrants must demonstrate particularized probable cause as to *every* user whose search

query data is searched and seized. *Ybarra v. Illinois*, 444 U.S. 85, 91–92 (1979) (“mere propinquity” to criminal activity insufficient to establish probable cause).

The keyword warrant in this case falls short of this requirement. Instead, it relies on what one court has called an “inverted probable cause argument—that law enforcement may seek information based on probable cause that some unknown person committed an offense, and therefore search every person present nearby.” *United States v. Chatrie* (“*Chatrie I*”), 509 F. Supp. 3d 901, 933 (E.D. Va. 2022), *affd en banc on other grounds*, 136 F.4th 100 *en banc* (4th Cir. 2025); *see also id* at 928 (citing *Maryland v. Pringle*, 540 U.S. 366, 371 (2003)). Similarly, the search here assumes that the unknown perpetrator searched for a particular term and the hunch is that no one else searched for that term, and that anyone who did is worthy of suspicion, regardless of where in the world they are.

Indeed, the lower court’s reasoning would support a keyword warrant to Google *whenever* an officer can articulate a hunch that records of a Google search would provide evidence relevant to a criminal investigation. The keyword warrant therefore did not demonstrate “particularized probable cause” as to these users. *Chatrie I*, 509 F. Supp. 3d at 929.

In addition, the warrant purported to authorize a broad search for information that (1) may not be relevant to the case and (2) would unreasonably disclose private information about third parties, if the search term happened to

reveal identities of users other than the perpetrator. It authorized disclosure of all IP addresses associated with the search terms, which is essentially identifying information about every user who searched for the address. *Search Warrant Attachment B*, category (a). It further demanded data showing any correlation between the IP addresses and any Google Accounts, including email, video conferencing, file storage, streaming video and chat/direct messaging accounts, none of which are relevant to the case and for which no probable cause was established. *Id.* category (d).

If, however, this Court holds that keyword search warrants are permissible under some circumstances, it should impose safeguards to limit invasions of constitutionally protected rights of privacy, association, and freedom of thought.

First, law enforcement should be required to aver in its warrant application that it has exhausted other less invasive means of identifying the suspect. This is a familiar requirement for police; in the wiretapping context, for example, a warrant application must include “a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous.” Va. Code Ann. §19.2-68(A)(3).

Second, reverse search warrants should be issued only when there is some objective indication that the suspect actually used a search engine, and the search

terms are uncommon and specific enough that no one other than the perpetrator is likely to have searched for them. “How to make a bomb,” the name of a victim, the location of a crime scene, or other details already known to the general public are terms likely to sweep in innocent people. The aim is to limit to the extent possible how much information law enforcement gathers about people who use search engines to access information about matters that are not inherently incriminating.

Third, keyword search warrants must further minimize the intrusion into the private lives of Internet users individuals by:

- Requiring “justification for the time period for which the records will be gathered.” *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. 2703(c), 2703(d) Directing AT & T, Sprint/Nextel, T-Mobile, Metro PCS, Verizon Wireless (“S.D.N.Y. Tower Dump Order”)*, 42 F. Supp. 3d 511, 519 (S.D.N.Y. 2014);
- Requiring that the time period be no longer than necessary to identify individuals connected to the alleged crime;
- Requiring that the search terms are as circumscribed as possible;
- Prohibiting investigation of identifiers and accounts without returning to the court to explain the reason for further investigation and to obtain authorization;
- Requiring that law enforcement present and follow a protocol for the acquisition, search, analysis, use, retention, and deletion of the potentially

voluminous information obtained, designed to limit to the fullest extent possible invasions into the privacy of people that do not have any role in the purported criminal offense. See *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d)*, 930 F. Supp. 2d 698, 702 (S.D. Tex. 2012 (imposing this requirement in the context of CSLI); *SDNY Tower Dump Order*, 42 F. Supp. 3d at 519 (same); *In re Application of the U.S. for an Order Pursuant To 18 U.S.C. §2703(d)*, No. 2:17-MC-51662, 2017 WL 6368665, at *2 (E.D. Mich. Dec. 12, 2017) (same). Approved protocols could involve using a filter team walled off from the primary investigators to examine data, for example to determine if searchers were from areas other than where the crime was committed

- Requiring prompt deletion of information about people not suspected of the crime under investigation, except to the extent that information must be retained to satisfy *Brady* and similar disclosure obligations to the defense. If not immediately deleted, courts should require that such data be segregated and stored securely in a manner off limits to investigative queries.

Fourth, the individuals whose personal information was swept up during the course of the criminal investigation should be notified by either Google or the government after such reasonable time that notification would not jeopardize the

ongoing criminal investigation. *See In re Search of Cellular Tel. Towers*, 945 F. Supp. 2d 769, 771 (S.D. Tex. 2013).

Fifth, the warrant return should detail the number of accounts or individuals with data returned from the search and the number of those individuals who are not suspected of the crime under investigation. This data should be made publicly available, as it will allow judges, lawmakers, and voters insight into how invasive these searches are in practice and whether additional safeguards are needed.

Without these safeguards, law enforcement could access an avalanche of personal information of almost everyone in the nation nearly at will. Such a panopticon is contrary to the vision of America embodied in the state and federal constitutions. This Court should act to protect Virginians against such a threat and hold, at a minimum, requires that law enforcement meet all of the above requirements for a warrant.

CONCLUSION

For the reasons stated above, this Court should reverse the lower court's decision denying Appellant's motion to suppress.

Dated: July 10, 2025

Respectfully submitted,

By: /s/ Matthew W. Callahan

CERTIFICATE OF SERVICE AND COMPLIANCE

I, Matthew W. Callahan, certify as follows:

(a) On July 10, 2025, an electronic copy of the Motion for Leave to File Amicus Brief was filed, via VACES with the Office of the Clerk, Court of Appeals of Virginia, 109 North Eighth Street, Richmond, VA 23219.

(b) One electronic copy of the Amicus Brief was served on July 10, 2025, via email upon:

Nassir Aboreden, Deputy Commonwealth's Attorney
1425 N. Courthouse Road, #5200
Arlington, VA 22201
naboreden@arlingtonva.us
Counsel for Appellee

and

Kelsey Bulger, Deputy Appellate Counsel
Virginia Indigent Defense Commission
1604 Santa Rosa Road, Suite 200
Richmond, Virginia 23229
kbulger@vadefenders.org
Counsel for Appellant

(c) This Amicus Brief contains 7,950 words in compliance with Rule 5A:19(a).

/s/ Matthew W. Callahan