

DENVER DISTRICT COURT
Address: 520 W. Colfax Ave., Denver, CO 80204

DATE FILED: July 1, 2022 11:40 AM
FILING ID: 50C69AB1D3BC3
CASE NUMBER: 2021CR20001

THE PEOPLE OF THE STATE OF COLORADO

v.

GAVIN SEYMOUR,
Juvenile Defendant.

Hannah Seigel Proff
Atty. Reg. # 40112
Proff Law, LLC
1563 N. Gilpin Street
Denver, Colorado 80218
Phone: 303-628-5581
Hannah@ProffLaw.com

Jennifer Lynch
Pro Hac Vice Atty. Reg # 22PHV7045
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Phone: 415-436-9333
jlynch@eff.org

I. ▲ COURT USE ONLY ▲

Case Number: 21CR20001

Div.: 5A

**BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION
IN SUPPORT OF DEFENDANT'S MOTION TO SUPPRESS**

TABLE OF CONTENTS

TABLE OF CONTENTS..... i

TABLE OF AUTHORITIES ii

INTERESTS OF AMICUS CURIAE..... 1

INTRODUCTION 1

BACKGROUND 3

 I. Keyword Search Warrants Draw on Vast Repositories of Data Held by Search Engines,
 Which Are Nearly Indispensable to Browsing the Internet. 3

 A. Search Engines Are Indispensable to Browsing the Internet..... 3

 B. Keyword Warrants Allow Access to Billions of Users’ Search Queries and Have
 the Potential to Implicate Innocent People. 8

ARGUMENT 12

 II. Keyword Warrants Are Unconstitutional General Warrants in Violation of the Fourth
 Amendment and Article II, Section 7..... 12

 III. Keyword Warrants Harm Expressive Freedoms and Cannot Survive Heightened Fourth
 Amendment Scrutiny..... 14

 A. The Keyword Warrant Compromises Expressive Freedoms..... 15

 B. Given the Expressive Freedoms Implicated by the Keyword Warrant, the Fourth
 Amendment Must Be Applied with “Scrupulous Exactitude.” 18

 IV. The Colorado Constitution Is Even More Protective than the Federal Constitution..... 18

CONCLUSION..... 21

TABLE OF AUTHORITIES

Cases

| | |
|-------------------------------------------------------------------------|-----------|
| <i>Andresen v. Maryland</i> , 427 U.S. 463 (1976) | 12 |
| <i>Bd. of Educ. v. Pico</i> , 457 U.S. 853 (1982) | 16 |
| <i>Bock v. Westminster Mall Co.</i> , 819 P.2d 55 (Colo. 1991) | 18 |
| <i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2018) | 14, 21 |
| <i>Ex parte Jackson</i> 96 U.S. 727 (1878) | 12 |
| <i>Kleindienst v. Mandel</i> , 408 U.S. 753 (1972) | 16 |
| <i>Lamont v. Postmaster Gen. of U.S.</i> , 381 U.S. 301 (1965) | 16, 17 |
| <i>Marron v. United States</i> , 275 U.S. 192 (1927) | 14 |
| <i>Martin v. City of Struthers, Ohio</i> , 319 U.S. 141 (1943) | 16 |
| <i>McIntyre v. Ohio</i> , 514 U.S. 334 (1995) | 17 |
| <i>Payton v. New York</i> , U.S. 573 (1980) | 15 |
| <i>People v. Coke</i> , 461 P.3d 508 (Colo. 2020) | 12 |
| <i>People v. McKnight</i> , 446 P.3d 397 (Colo. 2019) | 18 |
| <i>People v. Muniz</i> , 597 P.2d 580 (Colo. 1979) | 12 |
| <i>Riley v. California</i> , 573 U.S. 373 (2014) | 12 |
| <i>Stanford v. Texas</i> , 379 U.S. 476 (1965) | 2, 15, 18 |

| | |
|--------------------------------------------------------------------------------------------------|---------------|
| <i>Stanley v. Georgia</i> , 394 U.S. 557 (1969) | 17 |
| <i>Talley v. California</i> , 362 U.S. 60 (1960) | 17 |
| <i>Tattered Cover, Inc. v. City of Thornton</i> , 44 P.3d 1044 (Colo. 2002) | <i>passim</i> |
| <i>United States v. Chatrie</i> , No. 3:19cr130, 2022 WL 628905 (E.D. Va. Mar. 3, 2022) | 10, 14 |
| <i>United States v. Jones</i> , 565 U.S. 400 (2012) | 12 |
| <i>United States v. Leary</i> , 846 F.2d 592 (10th Cir. 1988) | 13 |
| <i>United States v. Playboy Entm't Grp., Inc.</i> , 529 U.S. 803 (2000) | 16, 17 |
| <i>United States v. Rumely</i> , 345 U.S. 41 (1953) | 17 |
| <i>United States v. Sells</i> , 463 F.3d 1148 (10th Cir. 2006) | 13 |
| <i>United States v. Van Leeuwen</i> 397 U.S. 249 (1970) | 12 |
| <i>Voss v. Bergsgaard</i> , 774 F.2d 402 (10th Cir. 1985) | 13 |
| <i>Ybarra v. Illinois</i> 444 U.S. 85 (1979) | 13 |
| <i>Zurcher v. Stanford Daily</i> , 436 U.S. 547 (1978) | 2, 18 |
| Statutes | |
| 18 U.S.C. § 2703(c) | 11 |
| Constitutional Provisions | |
| CO. Const. art. II, § 10 | <i>passim</i> |
| CO. Const. art. II, § 7 | 2, 12, 21 |
| U. S. Const. amend. I | 2, 14, 15 |
| U.S. Const. amend. IV | <i>passim</i> |

Other Authorities

| | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
| Aaron Mackey, et al., EFF, <i>Unreliable Informants: IP Addresses, Digital Tips and Police Raids</i> (Sept. 2016) | 11 |
| Danny Sullivan, <i>How Autocomplete Works in Search</i> , Google (Apr. 20, 2018)..... | 6 |
| Danny Sullivan, <i>How Google Autocomplete Predictions Are Generated</i> , Google (Oct. 8, 2020). | 5 |
| David Nield, <i>A Guide to Using Android Without Selling Your Soul to Google</i> , Gizmodo (July 26, 2018)..... | 8 |
| <i>Global requests for user information—United States</i> , Google..... | 8 |
| <i>Google Searches in 1 Second</i> , Internet Live Stats | 6 |
| <i>How Google Search Works</i> , Google | 4 |
| <i>How To Find The IP Address Of A Website</i> , WhatIsMyIP.com..... | 3 |
| Jennifer Valentino-DeVries, <i>Tracking Phones, Google Is a Dragnet for the Police</i> , N.Y. Times (Apr. 13, 2019) | 8 |
| Luke Johnson, <i>How to See EVERY Google Search You’ve Ever Made</i> , Digital Spy (Dec. 27, 2016)..... | 7 |
| Maryam Mohsin, <i>10 Google Search Statistics You Need to Know</i> , Oberlo (Jan. 2, 2022) | 6, 7 |
| <i>May 2022 Web Server Survey</i> , Netcraft (May 30, 2022)..... | 3 |
| Michael Arrington, <i>AOL Proudly Releases Massive Amounts of Private Data</i> , TechCrunch (Aug. 6, 2006)..... | 5 |
| Michael Barbaro & Tom Zeller Jr., <i>A Face Is Exposed for AOL Searcher No. 4417749</i> , N.Y. Times (Aug. 9, 2006)..... | 5 |
| 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) | 10 |
| <i>Search Engine Market Share in 2022</i> , Oberlo | 6 |
| Siladitya Ray, <i>Google Shared Search Data With Feds Investigating R. Kelly Victim Intimidation Case</i> , Forbes (Oct. 8, 2020)..... | 9 |
| <i>Supplemental Information on Geofence Warrants in the United States</i> , Google (2021)..... | 9 |
| <i>The Most Asked Questions on Google</i> , Mondovo..... | 5 |
| Thomas Brewster, <i>Cops Demand Google Data on Anyone Who Searched a Person’s Name... Across a Whole City</i> , Forbes (Mar. 17, 2017) | 8, 9 |
| Thomas Brewster, <i>Exclusive: Government Secretly Orders Google to Identify Anyone Who Searched A Sexual Assault Victim’s Name, Address or Telephone Number</i> , Forbes (Oct. 4, 2021)..... | 9 |
| Vangie Beal, <i>Dynamic URL</i> , Webopedia (May 24, 2021) | 4 |

| | |
|------------------------------------------------------------------|---|
| <i>View & control activity in your account, Google</i> | 7 |
| <i>Web crawler, Wikipedia (June 26, 2022)</i> | 4 |
| <i>Year in Search 2021, Google</i> | 5 |

INTERESTS OF AMICUS CURIAE

The Electronic Frontier Foundation (“EFF”) is a non-profit, member-supported digital civil liberties organization. Founded in 1990, EFF has over 35,000 active donors and dues-paying members across the United States, including in the state of Colorado. EFF represents the interests of technology users in court cases and broader policy debates surrounding the application of law to technology and defends the right to be free from the government’s use of technology to conduct unreasonable searches and seizures. EFF regularly participates both as direct counsel and as amicus in the Supreme Court, the Colorado Supreme Court, and other state and federal courts in cases addressing the Fourth Amendment and its application to new technologies. *See, e.g., Carpenter v. United States*, 138 S. Ct. 2206 (2018); *Riley v. California*, 573 U.S. 373 (2014); *People v. Tafoya*, 494 P.3d 613 (Colo. 2021).

EFF’s interest in this case is in the preservation of federal and state constitutional guarantees against unreasonable government intrusions into private life and associations and into protected expressive speech.

INTRODUCTION

The Internet is crucial to our understanding of and engagement with the world. But it can be nearly impossible to navigate the billions of sites on the Web and find relevant information without the use of a search engine like Google. Many users have come to rely on search engines to such a degree that they routinely search for the answers to sensitive or unflattering questions that they might never feel comfortable asking a human confidant—even friends, family members, doctors, or clergy. Yet as has become clear in this case, Google retains detailed information on the search queries of everyone who uses its search engine. Over the course of

months and years, there is little about a users' life that will not be reflected in their search keywords, from the mundane to the most intimate. The result is a vast record of some of users' most private and personal thoughts, opinions, and associations.

Because of the breadth and detailed nature of search query data, the use of keyword search warrants by law enforcement is especially concerning. Keyword search warrants are unlike typical warrants for electronic information in a crucial way: they are not targeted to specific individuals or accounts. Instead, they require a provider to search its entire reserve of user data—in this case the queries of one billion Google users—and identify any and all users or devices that searched for words or phrases specified by law enforcement. As in this case, the police generally have no identified suspects when they seek a keyword search warrant. Instead, the sole basis for the warrant is the officer's hunch that the suspect might have searched for something in some way related to the crime.

Keyword warrants are dragnet searches that violate the First and Fourth Amendments to the U.S. Constitution and Article II, Sections 7 and 10 of the Colorado Constitution. Like the 18th century writs of assistance that inspired the Fourth Amendment's drafters, these warrants are especially pernicious because 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). For this reason, they must be examined with heightened scrutiny. *Zurcher v. Stanford Daily*, 436 U.S. 547, 564, 565 (1978); *Tattered Cover*, 44 P.3d at 1057. Because the warrant in this case targets speech, lacks probable cause to support a search of a billion Google users'

search queries, and is therefore unconstitutionally overbroad, Amicus urges this Court to grant Defendant’s motion to suppress all evidence generated from the warrant.

BACKGROUND

I. Keyword Search Warrants Draw on Vast Repositories of Data Held by Search Engines, Which Are Nearly Indispensable to Browsing the Internet.

A. Search Engines Are Indispensable to Browsing the Internet.

Keyword warrants are possible because, on the Internet, it is virtually impossible to find a website or any other information without entering search terms (also known as “keywords”) into a search engine. According to some sources, there are over 1.15 billion websites, and tens of billions of webpages.¹ Much as houses and businesses have street addresses in the physical world, the servers that host websites are associated with a numerical address as well. These addresses, known as “Internet Protocol” or IP addresses, are a series of numbers that represent the server or computer where a website is hosted. For example, one of Google.com’s IP addresses is 173.194.215.99.² Because IP addresses are difficult to remember, domain names like “google.com” serve as user-friendly stand-ins. However, to navigate to a specific *page* within a website, one would need a link to not just the domain name but also the exact URL (“uniform resource locator”) for that webpage. For example, the domain for the Colorado state courts

¹ *May 2022 Web Server Survey*, Netcraft (May 30, 2022), <https://news.netcraft.com/archives/category/web-server-survey>; “The size of the World Wide Web (The Internet),” Tilburg University, <https://www.worldwidewebsite.com/>. Websites can contain any number of individual webpages.

² IP addresses are not necessarily static and may change. They can be identified using a command line prompt or a simple lookup tool such as <https://www.whatismyip.com/dns-lookup>. See *How To Find The IP Address Of A Website*, WhatIsMyIP.com, <https://www.whatismyip.com/how-to-find-the-ip-address-of-a-website>.

website is [courts.state.co.us](https://www.courts.state.co.us), and the specific URL for the Denver County courts web page is https://www.courts.state.co.us/Courts/County/Index.cfm?County_ID=3. URLs may be quite long and can even be “dynamic,” generated from specific user queries to a site’s database, such as in response to a search on Google or Amazon.³ For example, to get directions to the Denver courthouse using Google Maps, one would need to enter <https://www.google.com/maps/dir//520+W+Colfax+Ave,+Denver,+CO+80204/@39.7393358,-105.064741,12z/data=!4m8!4m7!1m0!1m5!1m1!1s0x876c78d2fb8e0a7d:0xab7d8a701106d34!2m2!1d-104.994701!2d39.7393568>—or just use a search engine.

Search engines make it possible to find not just the website a person is looking for, but also specific content within that website, including text, video, images, and pdfs. 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 relevancy to a search query.⁴

The keywords that users type into search engines can be incredibly revealing of their most intimate and private thoughts, ideas, and concerns. Internet users frequently search for answers to pressing medical questions for themselves and loved ones, information about world events and controversial ideas, discussions of gender and sexuality, and directions on how to get to various places, to give just a few examples out of the nearly limitless possibilities. Specialized users may search for seemingly more “incriminating” information; a crime novelist could search

³ Vangie Beal, *Dynamic URL*, Webopedia (May 24, 2021), https://www.webopedia.com/TERM/D/dynamic_URL.html.

⁴ *Web crawler*, Wikipedia (June 26, 2022), https://en.wikipedia.org/wiki/Web_crawler; *How Google Search Works*, Google, <https://www.google.com/search/howsearchworks/how-search-works>.

for unique ways to kill people, a historian of the civil rights era could search for racist language, or a policy analyst could search for specifics on how drugs are manufactured and used. Some of the top questions posed to Google are “how to register to vote,” “how to get pregnant,” “how to have sex,” and “how to be happy alone.”⁵ Even a simple query for an address can be revealing. For example, knowing that a person searched for “7155 E 38th Ave, Denver,” could lead to an inference that the person was seeking an abortion. (This is the address of Planned Parenthood.) Searches can be so specific to an individual that even the most innocuous queries can quickly reveal who that person is. In 2006, AOL published three months of de-identified search history data from 650,000 users.⁶ 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.”⁷

Under some circumstances, the search queries that users enter may differ from those they originally intended. Modern search engines provide users with a feature called “autocomplete,” which relies on sophisticated algorithms to make predictions about what the user might be looking for based on data like the user’s geographic location, other things they have searched for in the past, their language, and “common and trending queries.”⁸ Search engines like Google

⁵ *The Most Asked Questions on Google*, Mondovo, <https://www.mondovo.com/keywords/most-asked-questions-on-google>; *Year in Search 2021*, Google, <https://trends.google.com/trends/yis/2021/US>.

⁶ 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>.

⁷ 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>.

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

provide a list of five to ten contextualized suggestions almost immediately after the user starts typing a query in the search bar, and those suggestions change as a user types in more letters.⁹ So, for example, a user in San Francisco, California, who types in “san” could immediately get suggestions for “San Francisco,” “San Francisco weather,” “San Francisco Giants,” and also “Sandra Bullock.” The user can click on any of the terms in the list to go straight to search results for that query. This feature can be particularly helpful and timesaving when searching on a mobile device’s smaller screen and letter keys. However, the ease with which a user can click on a predicted search term can also lead to users entering queries they never intended. This may be particularly true with less-common queries, such as addresses.

Google Search is far and away the most popular search engine, with 92.49% worldwide market share (87.72% in the United States),¹⁰ and “more than 1 billion average monthly users.”¹¹ Most people use Google to search the Internet at least 3 times per day,¹² and Google reportedly processes approximately 100,000 search queries every second.¹³ This translates to over 8.5

⁹ Danny Sullivan, *How Autocomplete Works in Search*, Google (Apr. 20, 2018), <https://www.blog.google/products/search/how-google-autocomplete-works-search>.

¹⁰ *Search Engine Market Share in 2022*, Oberlo, <https://www.oberlo.com/statistics/search-engine-market-share>.

¹¹ Declaration of Nikki Adeli ¶ 4 (hereinafter “Google Decl.”).

¹² Maryam Mohsin, *10 Google Search Statistics You Need to Know*, Oberlo (Jan. 2, 2022), <https://www.oberlo.com/blog/google-search-statistics>.

¹³ *Google Searches in 1 Second*, Internet Live Stats, <https://www.internetlifestats.com/one-second/#google-band>.

billion searches per day.¹⁴ As of 2019, 63% of those searches were conducted on mobile devices.¹⁵

Due to its market dominance and the importance of search engines to using the Internet, Google possesses massive amounts of information about users' searches. For Google 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.¹⁶ Google now allows users to delete their search history and to turn off Google's collection of that data.¹⁷ However, if 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.¹⁸

Even turning off Google's collection of search history data does not stop Google from tracking search queries; it only divorces that collection from other details in a user's account. As this case reveals, Google retains data on *anyone* who uses its search engine, not just Google users who are logged into their accounts. Google links searches to a device's IP address and Internet service provider and, using that information, an officer can easily "track that back and relate that

¹⁴ Mohsin, *supra* n.12.

¹⁵ *Id.*

¹⁶ See *View & control activity in your account*, Google, <https://support.google.com/accounts/answer/7028918>.

¹⁷ *Id.*

¹⁸ Luke Johnson, *How to See EVERY Google Search You've Ever Made*, Digital Spy (Dec. 27, 2016), <https://www.digitalspy.com/tech/a805172/how-to-see-every-google-search-youve-ever-made>.

search” to a specific person.¹⁹ Given this, it is very difficult to search Google anonymously. This is true whether users are searching using a personal computer or a handheld device like a phone.²⁰ It is unclear how long Google retains search history data from people who are not logged into Google accounts, but if it is anything like other data Google collects on users, Google’s database could go back a decade or more.²¹

B. Keyword Warrants Allow Access to Billions of Users’ Search Queries and Have the Potential to Implicate Innocent People.

The use of keyword search warrants is relatively new—the first press report of their use was in 2017²²—and it is unclear how many are issued each year. Google produces public reports that include the total number of warrants it receives every six months, but it does not break out the number of keyword warrants.²³ If keyword warrants are anything like another novel dragnet

¹⁹ Prelim. Hr’g Tr. 197:7–10, Nov. 12, 2021 (Testimony of Special Agent Mark Sonnendecker).

²⁰ 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>.

²¹ Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. Times (Apr. 13, 2019), <https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html> (noting at the time of the article that Google’s Location History data goes back nearly a decade).

²² 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>.

²³ See *Global requests for user information—United States*, Google, https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests,accounts;authority:US;time:&lu=user_requests_report_period.

method used to identify suspects—“geofence warrants”²⁴—their use is likely increasing year over year as more police agencies around the country learn about them. Geofence warrants now make up 25% of all warrants Google receives, and in Colorado, the number of geofence warrants increased by a factor of more than 10 between 2018 and 2020.²⁵

While several known keyword warrants have, as in this case, sought to identify everyone who searched for a specific address,²⁶ in other cases police have asked Google for everyone who searched for variations of a victim’s name or the name of someone else related to the case.²⁷ In at least two cases, the search queries have been far broader. In response to a series of pipe bombs in Austin, Texas, police sought everyone who searched for words like “low explosives” and “pipe bomb.”²⁸ And in Brazil, Google is currently challenging a warrant that sought identifying information for everyone who searched for the name of a popular politician who was

²⁴ Geofence warrants, also known as reverse location searches, seek information on every device that might have been within designated geographic areas and time periods in the past. Like keyword warrants, geofence warrants do not identify in advance any specific target device.

²⁵ *Supplemental Information on Geofence Warrants in the United States*, Google, 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). This document shows that police in Colorado sought 27 geofence warrants in 2018, 164 geofence warrants in 2019, and 308 geofence warrants in 2020.

²⁶ 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>.

²⁷ Brewster, *Cops Demand Google Data On Anyone Who Searched A Person’s Name... Across A Whole City*, *supra* n.22; 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), <https://www.forbes.com/sites/thomasbrewster/2021/10/04/google-keyword-warrants-give-us-government-data-on-search-users/?sh=545cc7b87c97>.

²⁸ Brewster, *Exclusive: Government Secretly Orders Google to Identify Anyone Who Searched a Sexual Assault Victim’s Name, Address or Telephone Number*, *supra* n.27.

assassinated, as well as the name of a cultural center and a well-trafficked street in Rio de Janeiro where the crime occurred.²⁹

It appears Google must search its entire database of users' search queries within the relevant time period to comply with a keyword warrant, including users well outside the area of the crime.³⁰ *See* Declaration of Nikki Adeli ¶ 4 (hereinafter Google Decl.) (stating that Google queries the records of users' searches conducted through Google Search and Maps to comply with a keyword warrant and noting that Google has on average one billion monthly users). This is because the warrant does not identify a particular account or device but instead seeks *any* device that may have searched for the terms specified by the officer during the relevant time period.

Google appears to have designed a multi-step approach to respond to keyword warrants. It states that it de-identifies the data provided in its initial response to police by “truncat[ing] account-identifying information in the results” and then provides “identifying information about responsive users” in a second step or in response to a second warrant. Google Decl. ¶¶ 7–9. However, in this case, Google provided enough information to allow the police to identify the source of search queries in the first step by providing full IP addresses in its initial production to Denver police. If police know the Internet service provider or carrier in addition to the IP

²⁹ 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>.

³⁰ *See United States v. Chatrle*, No. 3:19cr130, 2022 WL 628905, at *4 (E.D. Va. Mar. 3, 2022) (“Google has to compare *all* the data in the Sensorvault [database] in order to identify users within the relevant timeframe of a geofence.”).

address,³¹ they do not need to rely on Google to determine the source of the search query; instead, they can submit a simple subpoena to the carrier for billing records—including name and address—associated with that IP address.³²

Given the fact that keyword warrants do not identify specific suspect devices but instead require Google to search its entire data repository, all keyword warrants have the potential to implicate innocent people who just happen to be searching for something an officer believes is somehow linked to the crime. For example, the warrant in this case sought everyone who searched for a specific address on “Truckee” street. However, there are streets named “Truckee” in several cities and towns in Colorado, as well as in Arizona, California, Idaho, and Nevada. Keyword warrants could also allow officers to target people based on political speech and by their association with others. Police used multiple geofence warrants to identify people at political protests in Kenosha, Wisconsin, and Minneapolis after police killings in those cities.³³ Similarly, with keyword warrants, officers could seek to identify everyone who searched for the location or the organizers of a protest.

³¹ It is possible to determine the ISP associated with an IP address using a simple lookup tool, such as <https://www.whatismyip.com/ip-address-lookup>.

³² Aaron Mackey, et al., EFF, *Unreliable Informants: IP Addresses, Digital Tips and Police Raids* 8 (Sept. 2016), https://www.eff.org/files/2016/09/22/2016.09.20_final_formatted_ip_address_white_paper.pdf; 18 U.S.C. § 2703(c)(2) (requiring providers to disclose certain customer records to law enforcement).

³³ 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>.

ARGUMENT

II. Keyword Warrants Are Unconstitutional General Warrants in Violation of the Fourth Amendment and Article II, Section 7.

The Denver Police Department’s warrant to Google for “any Google accounts” that searched for specific addresses during the fifteen days preceding the crime is an unconstitutional general warrant. General warrants, which permit “a general, exploratory rummaging in a person’s belongings,” are prohibited by both the Fourth Amendment and the Colorado Constitution. *Andresen v. Maryland*, 427 U.S. 463, 480 (1976); *People v. Coke*, 461 P.3d 508, 516 (Colo. 2020). They “are as objectionable today as they were when the Federal Constitution was drafted.” *People v. Muniz*, 597 P.2d 580, 582 (Colo. 1979) (en banc).

Data that can reveal sensitive, personal, and private details about a person—like keywords—can only be seized and searched with a warrant. *See Riley v. California*, 573 U.S. 373, 396 (2014) (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) and requiring a warrant to search a cell phone because it contains “a wealth of detail about [a person’s] familial, political, professional, religious, and sexual associations”). That warrant must satisfy all the Fourth Amendment’s familiar requirements—that it be issued by a neutral and detached judicial officer, supported by probable cause, and describe with particularity the place to be searched and the items to be seized. *See Ex parte Jackson*, 96 U.S. 727, 733 (1877); *United States v. Van Leeuwen*, 397 U.S. 249, 251 (1970).

The keyword warrant in this case fails each of these requirements. The warrant lacks particularity because it does not identify any specific person or profile to be searched. It is overbroad because it asked Google to search through the private data of a billion users. *United*

States v. Leary, 846 F.2d 592, 601–02, 606 (10th Cir. 1988) (search warrant is “impermissibly overbroad” if it “contains no limitation on the scope of the search”). And the warrant cannot be supported by probable cause because there are no facts indicating that any particular person in Google’s database was in any way personally connected to the crime. *Id.* at 605 (“a search warrant is also impermissibly overbroad if it authorizes the search and seizure of evidence that is not supported by probable cause”). The mere possibility that the perpetrator might have searched for the address of the scene of the crime sometime before the crime occurred is insufficient to support probable cause to search through *all* users’ data.³⁴ See *Ybarra v. Illinois*, 444 U.S. 85, 91–92 (1979) (“mere propinquity” to criminal activity insufficient to establish probable cause).

In effect, this warrant gave law enforcement authorization to conduct a digital dragnet search through the search history of a billion Google users; and it gave the police the authority and discretion to require Google to produce more information about particular devices that the police, alone, deemed of interest. By starting with a broad search that seeks information from *all* accounts that might have searched for a specific term, keyword warrants give the police unrestricted license to search each of those accounts and then, without clear limiting criteria or further judicial oversight, to conduct a more detailed search of a subset of those accounts. This is

³⁴ Neither the convenience of gathering information on all individuals nor the fact that a broad warrant such as this one might return some information relevant to the investigation—and might therefore be “particular” as to that information—can justify a warrant after the fact or in any event allow that particular or particularly helpful information to be severed and introduced. See, e.g., *Leary*, 846 F.2d at 600 (citing *Voss v. Bergsgaard*, 774 F.2d 402, 404 (10th Cir. 1985)) (categorical descriptions in warrant failed to “ensure that [the] search is confined in scope to particularly described evidence relating to a specific crime for which there is demonstrated probable cause”); *United States v. Sells*, 463 F.3d 1148, 1158 (10th Cir. 2006) (noting severance cannot “sav[e] a warrant that has been rendered a general warrant by nature of its invalid portions despite containing some valid portion”).

in direct contrast to a valid search warrant, where “[n]othing is left to the discretion of the officer executing the warrant.” *Marron v. United States*, 275 U.S. 192, 196 (1927).³⁵ Keyword warrants are, instead, modern general warrants.

The warrant here is arguably even broader than the general warrants and “writs of assistance” that inspired the Fourth Amendment’s drafters because it is not necessarily limited by physical geography or officer manpower. It provides officers a window into the search queries of a billion Google users—search queries that were entered well before the investigation ever began or the crime even occurred. A warrant like this was not conceivable or possible 20 years ago, much less at the nation’s founding, and it “gives police access to a category of information otherwise unknowable.” *Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018).

The breadth of the warrant here, coupled with the absence of specific information about the accounts or devices to be searched, renders it invalid under the Fourth Amendment.

III. Keyword Warrants Harm Expressive Freedoms and Cannot Survive Heightened Fourth Amendment Scrutiny.

The keyword search warrant does not just authorize indiscriminate interference with privacy rights, it also compromises protections for expressive freedoms guaranteed by the First Amendment and Article II, Section 10 of the Colorado Constitution.

Cases like this one that involve the intersection of expressive freedoms and government searches directly motivated the Framers’ disapproval of general warrants and the adoption of the

³⁵ Even if Google, rather than the police, insists on narrowing the identified suspects at the second step, this is insufficient to save an otherwise unconstitutional warrant. As a federal district court held recently in reviewing a geofence warrant issued to Google, “Fourth Amendment protections should not be left in the hands of a private actor.” *Chatrue*, 2022 WL 628905, at *25 n.44.

Fourth Amendment. 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 v. Texas*, 379 U.S. 476, 482 (1965). 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) (“decisions granting recovery to parties arrested or searched under general warrants on suspicion of seditious libel” were “fresh in the colonists’ minds”).

The fact that this warrant threatens protections guaranteed by the First Amendment and Article II, Section 10—including the freedom of speech, freedom of press, and freedom of association—reinforce the conclusion that the warrant violates the Fourth Amendment and its Colorado counterpart.

C. The Keyword Warrant Compromises Expressive Freedoms.

By targeting Google users’ search queries, the keyword warrant is directed entirely at expressive activity, beginning with the literal words of the targeted queries. Because search engines are an indispensable tool for finding information on the Internet, querying a search engine implicates not just the First Amendment’s well-known protection for the freedom of speech, but also the rights to distribute and receive information, and to freely and privately associate with others.

The U.S. Supreme Court has repeatedly held 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 op.); *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 of Struthers*, 319 U.S. 141, 146-47 (1943) .”) (“Freedom to distribute information to every citizen wherever he desires to receive it is so clearly vital to the preservation of a free society that . . . it must be fully preserved. The Colorado Supreme Court agrees. *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1051 (Colo. 2002) (en banc), *as modified on denial of reh’g* (Apr. 29, 2002) (right to receive, “though not explicitly articulated in either the Federal or Colorado Constitution, [is] necessary to the successful and uninhibited exercise of the specifically enumerated right to ‘freedom of speech’”). A speaker’s exercise of the freedom to speak and 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.” *Id.* (emphasis added). 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. and Colorado Supreme Courts have expressed special concern for attempts by the government to discover people’s interest in specific reading material. *See Stanley*, 394 U.S. at 565; *Tattered Cover*, 44 P.3d at 1051. Searches of places such as bookstores and libraries that allow people to search for and access reading material are especially disfavored. “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.” *United States v. Rumely*, 345 U.S. 41, 57 (1953) (Douglas, J., concurring). 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); *Talley v. California*, 362 U.S. 60, 64–65 (1960)).

Investigations of users’ online search queries raise identical concerns to 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 rights 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 (holding unconstitutional a requirement that readers affirmatively request to receive their own communist political mail); *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”).

D. Given the Expressive Freedoms Implicated by the Keyword Warrant, the Fourth Amendment Must Be Applied with “Scrupulous Exactitude.”

The keyword warrant’s substantial impact on expressive freedoms only compounds the many Fourth Amendment deficiencies described above and in Defendant’s Motion to Suppress. When a government search directly implicates expressive activity, the U.S. Supreme Court has 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 v. Stanford Daily*, 436 U.S. 547, 565, 564 (1978) (quoting *Stanford*, 379 U.S. at 485). Given the substantial discretion left to agents executing the keyword warrant in this case, as well as the impossibility of demonstrating probable cause to support a search through the query history of hundreds of millions of innocent Google users, it is clear these preconditions were not met with anything approaching scrupulous exactitude.

IV. The Colorado Constitution Is Even More Protective than the Federal Constitution.

Even if the Fourth Amendment could be satisfied in this case—and it cannot—Article II, Section 10 provides additional grounds to find the warrant unconstitutional. The Colorado state constitution affords stronger protections against both unlawful searches and seizures and against government intrusions on expressive activity. *People v. McKnight*, 446 P.3d 397, 406–07 (Colo. 2019) (Colorado Constitution “impos[es] more stringent constraints on police conduct than does the Federal Constitution.” (citations omitted)); *Bock v. Westminster Mall Co.*, 819 P.2d 55, 59–60 (Colo. 1991) (en banc) (recognizing state’s extensive history of affording broader protection for expressive rights under the state constitution).

In some cases, a specific, limited search or seizure may be described in a warrant that satisfies the “scrupulous exactitude” standard under the Fourth Amendment. Yet under Article II, Section 10, “the substantial chilling effects that could occur if this hypothetical search warrant were executed” require that “the police should be entirely precluded from executing the warrant.” *Tattered Cover*, 44 P.3d at 1055–56. This is especially true where the government’s warrant is based on the content of the information sought by the customer. *Id.* at 1059. Because the warrant in this case sought everyone who searched for specific keywords and compromised untold numbers of Google users’ expressive freedoms, this is such a case.

In *Tattered Cover*, the Colorado Supreme Court considered a bookstore’s preenforcement challenge to a warrant authorizing a search of the bookstore for evidence in a drug investigation. 44 P.3d at 1048. State and federal agents identified four suspects living in a trailer and discovered evidence of “drug operations” and a mailer addressed to “Suspect A” from the Tattered Cover bookstore in some trash from the trailer. *Id.* Acting on a warrant, they searched the trailer and found evidence of a meth lab, as well as two books with instructions on manufacturing drugs. *Id.* at 1048–49. The lead officer then sought a search warrant for Tattered Cover’s customer records in the hopes of linking Suspect A to the instructional books. *Id.* at 1049. The bookstore refused to comply. *Id.*

In holding that the Tattered Cover warrant was invalid, the supreme court took note of the substantial harm to the expressive rights of the bookstore and its patrons that would result from the search. “The dangers, both to Suspect A and to the book-buying public, of permitting the government to access the information it seeks, and to use this proof of purchase as evidence of Suspect A’s guilt, are grave.” 44 P.3d at 1063. Taking note of the long line of U.S. Supreme

Court cases protecting the right to receive information, the court explained that the Colorado Constitution has been interpreted to provide even broader protections, including the right to buy books anonymously. *Id.* at 1052–54. As a result, the court imposed a heightened standard of review above and beyond the Fourth Amendment’s warrant requirement: “law enforcement officials must demonstrate a sufficiently compelling need . . . *for the precise and specific information sought.*” *Id.* at 1058 (emphasis original). This standard includes a consideration of whether the intrusion was “limited in scope so as to prevent exposure of other constitutionally protected materials.” *Id.*

Applying this test, the court refused to enforce the Tattered Cover warrant. It noted that the very reason that the government sought the information—tying Suspect A to the content of the books—was “precisely the reason” the warrant was “likely to have chilling effects on the willingness of the general public to purchase books about controversial topics.” 44 P.3d at 1063. Even if the suspect were shown to have purchased the books, he might have done so for “any of a number of reasons, many of which are in no way linked to his commission of any crime,” including buying them for a friend or out of idle curiosity. *Id.* And even if these explanations were less likely than the government’s, “Colorado’s long tradition of protecting expressive freedoms cautions against permitting the City to seize the Tattered Cover’s book purchase record.” *Id.*

This Court should find that the keyword warrant in this case fails the standards of Article II, Section 10 for the reasons articulated in *Tattered Cover*. Like customers of a bookstore, users seek out information of every sort from search engines like Google. *See supra* Section I.A. Many queries reflect individuals’ most private thoughts, political and spiritual beliefs, and intimate and

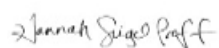
personal details about themselves. Search queries are also not infrequently attempts to satisfy idle or eccentric curiosity that the searcher would otherwise never express publicly. The purported probable cause supporting the keyword warrant assumes that if a person searched for that address of the crime scene, they are likely to have committed the crime. Just as in the *Tattered Cover* case, individuals who ran the queries targeted in the keyword warrant could have had any number of motivations to do so, unrelated to any crime.

However, the scope of the keyword warrant in this case is far broader than the *Tattered Cover* warrant. In *Tattered Cover*, the police sought to link the book purchase to a single pre-identified suspect, whereas here, the warrant named no suspects at all. This dragnet search therefore raised the possibility of sweeping in many more innocent individuals. Hence, the “exposure of other constitutionally protected materials” is even greater, and the government’s need for the “specific information sought”—the unbounded results of its warrant—is correspondingly insufficient. *Tattered Cover*, 44 P.3d at 1058.

CONCLUSION

For the reasons above and in keeping with the intent of the Framers to protect against “too permeating police surveillance,” *Carpenter*, 138 S. Ct. at 2214, Amicus respectfully urges the Court to hold that this keyword warrant violates the both the Fourth Amendment and Article II, Section 7 and to suppress all evidence.

Dated this day: July 1, 2022



Attorney: Hannah Seigel Proff, Atty. Reg. # 40112

Hannah Seigel Proff
Proff Law, LLC
1563 N. Gilpin Street
Denver, Colorado 80218
Phone: 303-628-5581
Hannah@ProffLaw.com

Jennifer Lynch
Pro Hac Vice Atty. Reg # 22PHV7045
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
415-436-9333
jlynch@eff.org

I hereby certify that on July 1, 2022 a true and correct copy of this amicus brief was served upon all counsel of record.

Hannah Seigel Proff

Hannah Seigel Proff, Esq.