SUPREME COURT, STATE OF COLORADO Colorado State Judicial Building 2 East 14th Avenue, Denver, CO 80203 IN RE: THE PEOPLE OF THE STATE OF COLORADO v. GAVIN SEYMOUR, Juvenile Defendant.	**COURT USE ONLY** Case No.: 2023SA12 Related Case Below: 21-CR-20001 (*People v. Gavin Seymour)* Denver District Court, Div.: 5A

Attorneys for Amicus Curiae Electronic Frontier Foundation

Hannah Seigel Proff
Atty. Reg. # 40112
Proff Law, LLC
309 N. Downing Street
Denver, Colorado 80205
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

BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF GAVIN SEYMOUR'S PETITION FOR REVIEW PURSUANT TO C.A.R. 21

CERTIFICATE OF COMPLIANCE

I hereby certify that this brief complies with C.A.R. 29 and C.A.R. 32, including all formatting requirements set forth in these rules.

Specifically, the undersigned certifies that

The amicus brief complies with the applicable word limit set forth in C.A.R. 29(d).

The amicus brief contains 4,732 words (does not exceed 4,750 words).

The amicus brief complies with the content and form requirements set forth in C.A.R. 29(c).

I acknowledge that my brief may be stricken if it fails to comply with any of the requirements of C.A.R. 29 and C.A.R. 32.

Hannah Seigel Proff, Atty. Reg. # 40112

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Constitutional Provisions

Other Authorities

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 Colorado. 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, this Court, and many others 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.

JURISDICTION

This case involves a novel legal question: whether the police can seek access to the search queries of *all* Google users on a mere hunch that the perpetrator of a crime might have searched Google for a term that could, in the eyes of police, be

connected to the crime. The trial court below refused to engage with this question and denied Defendant's motion to suppress from the bench with no written order.

This Court should exercise its original jurisdiction pursuant to C.A.R 21 and address this question. Because warrants like the one at issue here target the protected speech of one billion Google users, including users well beyond Colorado's borders, and because no court has yet to address the constitutionality of such warrants, this case "raise[s] issues of significant public importance that [the Court has] not yet considered." *Wesp v. Everson*, 33 P.3d 191, 194 (Colo. 2001). Because an appellate remedy would also be inadequate, *id*., amicus urges this court to grant Petitioner's requested relief pursuant to C.A.R. 21.

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 websites 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. 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 user's 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, police use of keyword search warrants 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 police. 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 related to the crime.

Keyword warrants are dragnet searches. Like 18th-century writs of assistance that inspired the Fourth Amendment's drafters, keyword warrants are general warrants that permit police to conduct "a general, exploratory rummaging in a person's belongings." *Andresen v. Maryland*, 427 U.S. 463, 480 (1976). They are therefore prohibited by both the Fourth Amendment and the Colorado Constitution. *Id.*; *People v. Coke*, 461 P.3d 508, 516 (Colo. 2020). And like those

writs, keyword 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, and is overbroad, it violates both the state and federal constitution and should have been suppressed.

ARGUMENT

I. Keyword Warrants Draw on Vast Repositories of Data Held by Search Engines.

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

[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.worldwidewebsize.com/.

houses and businesses have street addresses in the physical world, servers that host websites are associated with a numerical address as well. These addresses, known as "Internet Protocol" or IP addresses, are series of numbers that represent the server or computer where a website is hosted. 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 website is 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," meaning they change based on users' search queries.[2] For example, to get directions to this Court using Google Maps, one would need to enter: https://www.google.com/maps/place/2+E+14th+Ave,+Denver,+CO+80203/@39.7372065,-104.9889931,17z/data=!3m1!4b1!4m5!3m4!1s0x876c7f2abe9bd2e1:0xe738e343b5d4e0c2!8m2!3d39.7372065!4d-104.9868044—or just use a search engine.

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

Search engines make it possible to find not just websites, but also specific content within websites, 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 search queries.[3]

The keywords that users type into search engines can be incredibly revealing. Internet users frequently search for specific addresses, answers to medical questions, information about controversial ideas, and discussions of gender and sexuality, 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 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 help abortion rights," "can I change my life," "how to get pregnant," and "how to have sex."[4] Even a simple query for an

---

[3] *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.

[4] *Year in Search 2022*, Google, https://trends.google.com/trends/yis/2022/US; *The Most Asked Questions on Google*, Mondovo, https://www.mondovo.com/keywords/most-asked-questions-on-google.

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 their identity. In 2006, AOL published three months of de-identified search history data from 650,000 users.[5] 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."[6]

Under some circumstances, users' search queries may differ from those they intended. Modern search engines offer an "autocomplete" feature, 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, their past search queries, their language, and "common and trending queries."[7] Search engines provide a list of

---

[5] 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.

[6] 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.

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

five to ten contextualized suggestions almost immediately after the user starts typing a query, and those suggestions change as a user types in more letters.[8] This feature can be particularly helpful when searching on a mobile device's smaller screen and letter keys. However, it can also lead to users entering unintended queries, which 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),[9] and "more than 1 billion average monthly users." *See* Seymour C.A.R. 21 Petition, Exh. 4, Decl. of Nikki Adeli ¶ 4 (hereinafter "Google Decl."). Most people use Google to search the Internet at least three times per day,[10] and Google reportedly processes approximately 100,000 search queries every second.[11] This translates to over 8.5

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

[9] *Search Engine Market Share in 2022*, Oberlo, https://www.oberlo.com/statistics/search-engine-market-share.

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

[11] *Google Searches in 1 Second*, Internet Live Stats, https://www.internetlivestats.com/one-second/#google-band.

billion searches per day.[12] As of 2019, 63% of those searches were conducted on mobile devices.[13]

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.[14] Google now allows users to delete search history and to turn off Google's collection of that data.[15] 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.[16]

Even turning off Google's data collection does not stop Google from tracking queries; it only divorces that collection from other details in a user's

---

[12] Mohsin, *supra* n.10.

[13] *Id.*

[14] *See View & control activity in your account*, Google, https://support.google.com/accounts/answer/7028918.

[15] *Id.*

[16] 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.

account. Google retains data on *anyone* who uses its search engine, not just Google users who are logged into their accounts. Google links each search to a device's IP address and Internet service provider and, using that information, an officer can easily connect that search to a specific person.[17] 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.[18] 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.[19]

[17] Seymour C.A.R. 21 Pet., Exh. 4 (Nov. 12, 2021 Prelim. Hr'g Tr.), 197:7–10 (Testimony of Special Agent Mark Sonnendecker).

[18] 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.

[19] 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 publication, Google's Location History data goes back nearly a decade).

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 2017[20]—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.[21] If keyword warrants are anything like another novel dragnet method used to identify suspects—"geofence warrants"[22]—their use is likely increasing year over year. 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.[23]

---

[20] 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.

[21] *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.

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

[23] *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).

Several known keyword warrants have, as in this case, sought to identify everyone who searched for a specific address.[24] However, in other cases police have investigated other search queries, such as everyone who searched for variations of a victim's name or the name of someone else related to the case.[25] In at least two known cases, the search queries have been far broader. In response to a series of bombings in Austin, Texas, police sought everyone who searched for words like "low explosives" and "pipe bomb."[26] And in Brazil, Google is challenging a warrant for 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.[27]

---

[24] *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.

[25] Brewster, *Cops Demand Google Data On Anyone Who Searched A Person's Name... Across A Whole City*, *supra* n.20; 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.

[26] Brewster, *Exclusive: Government Secretly Orders Google to Identify Anyone Who Searched a Sexual Assault Victim's Name, Address or Telephone Number*, *supra* n.25.

[27] 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.

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. *See* Google Decl. ¶ 4. This is because the warrant does not identify a particular account or device but instead seeks *any* device that may have searched for the specified terms during the relevant time period. Further, although Google appears to have designed a multi-step approach to respond to keyword warrants that would seem to protect innocent users' identities, s*ee* Google Decl. ¶¶ 7–9 (describing process), at least in this case Google provided enough information in the first step—full IP addresses—to allow the police to identify the source for each of the search queries. If police know the ISP or carrier in addition to the IP address,[28] they do not need 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.[29]

Because keyword warrants require Google to search its entire data repository, they have the potential to implicate innocent people who happen to

---

5, 2022), https://www.eff.org/deeplinks/2022/04/google-fights-dragnet-warrant-users-search-histories-overseas-while-continuing.

[28] 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.

[29] *See* 18 U.S.C.§ 2703(c)(2).

search for something an officer believes is incriminating. For example, the warrant in this case sought everyone who searched for a specific address on "Truckee" street. However, there are "Truckee" streets 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.[30] Similarly, with keyword warrants, officers could seek to identify everyone who searched for the location or the organizers of a protest.

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

Keyword warrants do not just authorize indiscriminate interference with privacy rights, they also compromise protections for expressive freedoms guaranteed by the First Amendment and Article II, Section 10 of the Colorado Constitution.

[30] 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-dragnets-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.

Cases like this one that involve the intersection of expressive freedoms and indiscriminate government searches directly motivated the drafting and adoption of the 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 Article II, Section 10.

A. 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 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 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). This Court has agreed. *Tattered Cover*, 44 P.3d at 1051 (right to receive 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. Supreme Court and this Court have expressed special concern for government attempts 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 look 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 this 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 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").

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

A keyword warrant's substantial impact on expressive freedoms only compounds the many Fourth Amendment deficiencies described above. 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 police executing the keyword warrant in this case, as well as the impossibility of demonstrating probable cause to support searching the query history of a billion innocent Google users, it is clear these preconditions were not met with anything approaching scrupulous exactitude.

III. 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, *People v. McKnight*, 446 P.3d 397, 406–07 (Colo. 2019), and against government intrusions on expressive activity, *Bock v. Westminster Mall Co.*, 819 P.2d 55, 59–60 (Colo. 1991) (en banc).

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*, this 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. An officer then sought a search warrant for Tattered Cover's customer records in the hopes of linking Suspect A to the books. *Id.* at 1049. The bookstore refused to comply. *Id.*

In holding that the Tattered Cover warrant was invalid, this 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 state 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: police "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 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.*

Applying *Tattered Cover*, this Court should grant review to find that the keyword warrant in this case fails the standards of Article II, Section 10. 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 other intimate and personal details. Search queries often represent 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 the crime scene address, they are likely to have committed the crime. Just as in *Tattered Cover*, individuals who ran the queries targeted in the keyword warrant could have had any number of motivations for doing so, unrelated to any crime.

The scope of the keyword warrant in this case is, in fact, 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

This case is one of first impression that clearly "raise[s] issues of significant public importance." *Wesp*, 33 P.3d at 194. As such, and 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 grant Petitioner's requested relief pursuant to C.A.R. 21.

Dated this day: January 11, 2023

/s/ Hannah Seigel Proff

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

Hannah Seigel Proff
Proff Law, LLC
309 N. Downing Street
Denver, Colorado 80205
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 January 11, 2023 a true and correct copy of this amicus brief was served upon all counsel of record.

Hannah Seigel Proff, Atty. Reg. # 40112.