DATE FILED: March 7, 2023 9:05 AM
FILING ID: B5D5890D1FE3C
CASE NUMBER: 2023SA12

SUPREME COURT, STATE OF COLORADO

2 East 14th Ave.
Denver, CO 80203

Original Proceeding under C.A.R. 21
District Court, Denver County, 21CR20001

IN RE:

THE PEOPLE OF THE STATE OF COLORADO,

Plaintiff,

v.

GAVIN SEYMOUR,

Defendant.

KEVIN E. MCREYNOLDS, Senior Appellate Deputy District Attorney*
500 Jefferson County Parkway
Golden, CO 80401-6002
Telephone: (303) 271-6800
E-Mail: kmcreyno@jeffco.us
Registration Number: 40978

Thomas Raynes, Executive Director, Colorado District Attorneys' Council
3600 S. Yosemite St., Ste. 200
Denver, CO 80237

*Counsel for Amicus Curiae the Colorado District Attorneys' Council

▲**COURT USE ONLY**▲

Case No. 23SA12

AMICUS BRIEF SUBMITTED BY THE COLORADO DISTRICT ATTORNEYS' COUNCIL

CERTIFICATE OF COMPLIANCE

I hereby certify that this petition complies with the requirements of C.A.R. 29 and 32, including the formatting requirements set forth by those rules.

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

It contains **4,748** 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)

The undersigned acknowledges that this amicus brief may be stricken for failing to comply with this Court's rules.

/s/Kevin E. McReynolds

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

PAGE

CASES

TABLE OF AUTHORITIES

OTHER AUTHORITIES

CONSTITUTIONAL PROVISIONS

INTERESTS OF AMICUS

The Colorado District Attorneys' Council ("CDAC") is a statutorily authorized statewide organization comprised of Colorado's elected district attorneys. The mission of CDAC is to promote, foster, and encourage the effective administration of criminal justice throughout Colorado.

CDAC has a substantial interest in the safety of our communities, the investigation of criminal offenses, and the proper use of new investigative tools, including judicially approved search warrants to query the databases of third parties like Google that Defendant and his amici challenge in this case.

INTRODUCTION

After exhausting every standard investigatory tool to find the three masked people who set the house fire that killed five Senegalese immigrants, police turned to a new one, a Google keyword search warrant. This finally led investigators to Defendant and his friends. Ironically, given the privacy claims raised, they targeted this non-descript residence for destruction because a location tracking application suggested an iPhone taken from one of them was at the victims' home.

Selectively ignoring the limits of the address-only keyword warrant and the realities of the anonymized database query responses it produced, Defendant and

his amici, EFF and EPIC, raise the alarm against "what if" scenarios and potential abuses of keyword warrants to urge this Court to adopt a categorial right to digital privacy and prohibit any conceivable use of this investigative tool. But these boogeymen do not exist and neither the Fourth Amendment nor the Colorado Constitution support broadly sweeping away any notions of reasonableness to proclaim the absolutist views of D.C. digital rights lobbyists.

The Constitution requires this Court to balance the need to protect the public and solve serious crimes with a limited search of digital information that users have affirmatively provided to a public search engine. And that balance barely suggests any search at all, let alone a constitutionally unreasonable one. Looking to first principles, the minimal privacy interests, the narrow intrusion, and the balance of interests all support the reasonableness of the address-only keyword search here – especially with the additional privacy protections inherent to the warrant process.

Even when indulging the hypothetical concerns about abortion rights or other expressive web searches that EFF and EPIC seek to inject into the discussion, this Court addressed such concerns in *Tattered Cover v. City of Thornton*.[1] If and when law enforcement seeks a keyword warrant that delves into expressive

[1] 44 P.3d 1044, 1059 (Colo. 2002).

materials, *Tattered Cover* would requires proof that a compelling need for the information outweighs the potential harms caused by such a search. But those expressive and content-specific standards are not relevant here. There is nothing expressive about looking up directions to a house one plans to burn down, and address-only database queries do not implicate the freedoms of access to expressive or controversial content the *Tattered Cover* test was designed to protect. *See id.* at 1059 ("The harm will likely be minimal if the law enforcement officials' reasons for wanting the book purchase record are entirely unrelated to the contents of the books").

The district court correctly rejected Defendant's suppression motion.

ARGUMENTS IN SUPPORT OF THE TRIAL COURT'S RULING

A. There is a limited privacy interest in search terms users affirmatively provide to a third party, knowing that information is collected and may be disseminated to the Government.

The ultimate inquiry when evaluating the constitutionality of a search is one of reasonableness because both the federal and Colorado Constitutions prohibit "unreasonable searches and seizures." *See* U.S. Const. amend. IV; Colo. Const. Art. II, §7. The starting point of this analysis is to consider the privacy interests implicated. Indeed, the question of whether a government intrusion even

constitutes a "search" turns on whether the party opposing it had a reasonable expectation of privacy. *See Kyllo v. United States*, 533 U.S. 27, 33 (2001) (a "search" in the constitutional sense occurs "when the government violates a subjective expectation of privacy that society recognizes as reasonable") (citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)); *accord People v. McKnight*, 2019 CO 36, ¶22. The *Katz* framework has two components that were subsequently defined to cover any subjective expectation of privacy that society is prepared to recognize as reasonable. *See California v. Ciraolo*, 476 U.S. 207, 211 (1986). "The existence of a legitimate expectation of privacy must be determined after examining all the facts and circumstances in a particular case." *People v. Shorty*, 731 P.2d 679, 681 (Colo. 1987); *accord Oliver v. United States*, 466 U.S. 170, 177 (1984) ("No single factor determines whether an individual legitimately may claim under the Fourth Amendment that a place should be free of government intrusion not authorized by warrant").

And while *Katz* itself clarified that the Constitution "protects people, not places," the location of a governmental intrusion remains important in assessing the scope of the privacy interest. Not all areas are equivalent. *See Katz*, 389 U.S. at 351 ("What a person knowingly exposes to the public, even in his own home or

office, is not a subject of Fourth Amendment protection"); *but cf. Shorty*, 731 P.2d at 682 (public exposure may diminish the reasonable expectation of privacy, but it does not necessarily eliminate the expectation altogether). The heart of the Fourth Amendment is the protection of the home; the physical intrusion of the home was the "chief evil" it was designed to prevent. *See United States v. U.S. Dist. Ct.*, 407 U.S. 297, 313 (1972); *Payton v. New York*, 445 U.S. 573, 601 (1980) ("the overriding respect for the sanctity of the home that has been embedded in our traditions since the origins of the Republic"); *accord McKnight*, ¶¶118-23 (Samour, J., dissenting) (recognizing the "unique protection afforded the interior of a home" and "*significantly*" diminished expectation of privacy in other areas).

Outside the home, people have lesser privacy interests. For example, caselaw regarding the searches of automobiles and related warrant exceptions are premised on people's reduced privacy interest in automobiles. *See, e.g., California v. Carney*, 471 U.S. 386, 392 (1985) (discussing how the mobility and regulation of automobiles necessarily lead to a reduced expectation of privacy in their contents); *South Dakota v. Opperman*, 428 U.S. 364, 367 (1976) ("the expectation of privacy with respect to one's automobile is significantly less than that relating to one's home or office"); *accord People v. Litchfield*, 918 P.2d 1099, 1105-06 (Colo.

1996). This is reflected in other warrantless intrusions, such as dog sniffs. While federal courts have found no expectation of privacy in public odors, even before *McKnight* this Court had held that a dog sniff could nevertheless constitute a search by intruding into a location that implicated a reasonable expectation of privacy, such as a locked safe. *See People v. Unruh*, 713 P.2d 370, 378-79 (Colo. 1986) (recognizing an expectation of privacy in a locked safe subjected to a dog sniff, though finding this "search" reasonable in light of the circumstances).[2]

Beyond location, the privacy interests implicated require an evaluation of the pervasiveness and scope of the information that is subjected to the governmental intrusion. In *Riley*, the Supreme Court recognized that the sheer scope of information contained in a person's phone and the broad array of personal and sensitive information within it distinguished a smartphone from other containers or papers a person might carry. *Riley v. California*, 573 U.S. 373, 392-97 (2014). Thus, despite the generally reduced expectations of privacy for items taken from a person incident to an arrest, that phones effectively contain more personal information than would be exposed from the search of a person's home made the

[2] Colorado's law regarding dog sniffs is unique. It previously abrogated *Unruh* on grounds that a dog sniff was not a "search" of any kind but then later abrogated that conclusion in *McKnight* when finding a state constitutional expectation of privacy as it related to the possession of marijuana based on voters' adoption of Amendment 64.

complete search of its contents too deep an invasion to be conducted without a warrant. *See id.* at 396-98. Similarly, the scope of the information, its passive collection, and the exhaustive surveillance made possible through digital tracking tools is why the Supreme Court found a warrant is required to download months of cell-site location information ("CLSI"). *See Carpenter v. United States*, 138 S.Ct. 2206, 2221-23 (2018) ("In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection . . . [t]he Government's acquisition of the cell-site records here was a search" and thus its access will generally require a warrant); *accord, e.g., People v. Tafoya*, 2021 CO 62, ¶36 ("[W]hen government conduct involves continuous, long-term surveillance, it implicates a reasonable expectation of privacy. Put simply, the duration, continuity, and nature of surveillance matter when considering all the facts and circumstances in a particular case").

Looking to these overarching constitutional privacy considerations for guidance as to the reasonableness of the Google keyword search at issue suggests, at most, a minimal privacy interest.

First, the facts and circumstances suggest Defendant had a limited privacy interest in the Google database information the People sought to query because

Google transparently stated it collected and disseminated this information. Google's privacy policy informed users that it collected their search inquiries. (*See* Pet. For Rule 21, Exhibit 11 p. 4 ("We collect information about your activity in our services . . . [which] may include Terms you search for")). Google also explained that it would disclose this user information to other businesses and to comply with any "legal process, or enforceable governmental request" or to [p]rotect against harm to . . . the public." (*See id.* p. 13.) This policy provided advance notice to all Google users that their web search requests would be collected and could then be disseminated to law enforcement when requested through a legal process – in this case a search warrant. Google also provided alternatives that would allow users to conduct private searches ("you can also choose to browse the web privately using Chrome in Incognito mode") and to view and delete the search information Google had collected. (*See id.* pp. 3, 10-11, 15.) Thus, the keywords users affirmatively provided to Google under these terms is categorically different from a locked safe or the interior of one's home.

Second, society has long recognized that public web searches are not private and this lack of privacy has been documented in the popular press for decades.[3] This has included Google-specific articles recounting how the company records users' keyword searches, its transparent policies about this data collection, and the tools Google provides for users to control or limit this collection.[4] This widely-known lack of privacy when one uses public search engines has, in turn, spawned a cottage industry for people seeking to search anonymously by using websites that act as a "middle-man" for Google searches or alternative privacy-focused search engines that compete with Google.[5] Taken together, these circumstances suggest a reduced expectation of privacy over keywords one affirmatively provides to a public search engine. And this is why the keyword search information obtained by

---

[3] *See* Time Magazine, *Everything About You is Being Tracked—Get Over it*, Joel Stein, Mar. 21, 2011, Vol. 188, No.11; *accord United States v. Jones*, 565 U.S. 400, 427 (2012) (Alito, J., concurring) ("[E]ven if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconciles themselves to this development as inevitable").

[4] Todd Haselton, *How to find out what Google knows about you and limit the data it collects*, CNBC (Dec. 6, 2017). Available at: https://www.cnbc.com/2017/11/20/what-does-google-know-about-me.html

[5] *See* Sayak Boral, *How to Perform a Google Search Anonymously*, Maketecheasier (Jul. 8, 2020); Georgina Prodhan, *Startpage launches anonymous Web search service*, Reuters (Jan. 28, 2010). Available at: https://www.maketecheasier.com/perform-google-search-anonymously/ & https://www.reuters.com/article/internet-privacy-startpage/startpage-launches-anonymous-web-search-service-idINLDE60R1HB20100128

a warrant presents a narrower scope of privacy interests than the passively collected CSLI addressed in *Carpenter*. There the Supreme Court declined to find a diminished privacy interest from users' "voluntary" exposure of CSLI to their phone carriers because carrying a phone was an indispensable part of modern life without alternatives and every activity on that phone passively and automatically generated CSLI. *See Carpenter*, 138 S.Ct. at 2220.

Web searches are different. Both Google and the anonymous search industry provide clear and freely available alternatives to providing collectable search term data to Google. While using search engines may be essential for participating in modern society, using public search engines that are known to collect your activity is not. Further, unlike the passive and automatic surveillance of a person's movements through CSLI, keyword data is generated by the users themselves when they affirmatively send that information to a third party like Google.[6]

Third, the shallow information revealed by a keyword database inquiry stands on the opposite side of the spectrum from the "pervasive" surveillance of the intricacies of private life central to the *Riley* and *Carpenter* decisions. Here, the

[6] The assumption of risk discussion in *Carpenter* focused on the third-party doctrine, which Colorado has declined to follow on state constitutional grounds. *See, e.g., People v. Sporleder*, 666 P.2d 135, 144 (Colo. 1983). The Fourth Amendment's assumption of risk analysis is nevertheless helpful in assessing the reasonableness of a claimed privacy interest and its scope.

warrant here sought a small and brief set of information, an anonymized list of devices that searched for the victims' address in the days before three masked people burned it down. This snapshot of information was further limited to those devices located in Colorado when law enforcement sought a subsequent warrant to de-anonymize this list to identify users. This is nothing like the "intimate window into a person's life" and their "familial, political, professional, religious, and sexual associations" that led the Supreme Court to find a reasonable expectation of privacy over CSLI and the contents of one's phone. *See Carpenter*, 138 S.Ct. at 2217-18 (citing *Riley*). There is a "world of difference between the limited types of personal information" Google pulled from its business records database when creating a de-identified list of devices "and the exhaustive chronicle of location information" passively and pervasively collected through CSLI. *See id.* at 2219.[7]

Put simply, the address-specific search information that Defendant affirmatively provided to Google implicates minimal privacy interests.

[7] The nature of the particular information sought also suggests a lessened privacy interest in light of the regulation of this user information. *See Carney*, 471 U.S. at 393. Google's Privacy Policy complies with the federal regulatory scheme and the Colorado Privacy Act that goes into effect this July. As with automobiles, users necessarily have a reduced expectation of privacy over data that is subject to a regulatory scheme that grants users rights like those described in Google's policies, to review and delete information they choose to keep private.

B. Address-only keyword database queries are minimally intrusive.

A separate but related consideration when assessing constitutional reasonableness is the intrusiveness of the government's method for seeking the evidence. While any intrusion into an area in which a party has a reasonable expectation of privacy is a "search," the relative intrusiveness of that "search" is constitutionally significant. *See, e.g., Birchfield v. North Dakota*, 579 U.S. 438, 461-64 (2016) (recognizing a constitutionally-significant distinction between the intrusiveness of breath and blood tests of suspected drunk drivers and that the minimal intrusion of a breath test could be conducted without a warrant); *United States v. Place*, 462 U.S. 696, 705, 707 (1983) (considering the "the nature and extent of the intrusion" in assessing the reasonableness of a public dog sniff).

For searches outside the home, less intrusive techniques are more likely constitutional even without a warrant. For example, caselaw regarding aerial surveillance has consistently cited the "very limited degree of intrusiveness" when upholding the use of helicopters to observe sheds or enclosed greenhouses. *See Florida v. Riley*, 488 U.S. 445, 452 (1989) (rejecting a Fourth Amendment suppression claim because there was no interference with the normal use of the greenhouse, no undue noise, wind, or dust and the fly-over did not reveal any

intimate details connected with the use of the home or curtilage); *Henderson v. People*, 879 P.2d 383, 390 (Colo. 1994) (finding a helicopter fly-over of a residence was minimally intrusive and did not constitute a search under the totality of the circumstances); *accord Ciraolo*, 476 U.S. at 213, 215 (upholding observations from an fly-over in part because they were made "in a physically nonintrusive manner"). This concept has been similarly applied in the aforementioned DUI context and other warrantless testing circumstances. *See Birchfield*, 579 U.S. at 461 (equating the minimal invasiveness of breath BAC testing to the "negligible" warrantless intrusion of a buccal swab to collect DNA) (citing *Maryland v. King*, 569 U.S. 435, 446 (2013)); *Skinner v. Ry. Lab. Executives' Ass'n*, 489 U.S. 602, 626 (1989) (recognizing the minimal invasiveness of breath testing).

The address-only Google keyword search warrant here caused a similarly "negligible" intrusion into Defendant's privacy interests. Unlike the intrusive search of a phone discussed in *Riley*, the keyword warrant did not intrude on the intimate details of Defendant's digital life or "rummage" through his search history or other uses of Google's search engine. Rather, it narrowly sought a list of devices

that searched for the address of the non-descript suburban residence that became the scene of the targeted arson/murder police were trying to solve.

The nexus between the narrow intrusion and law enforcement's probable cause showing that the people who set this fire would have had to look up its location also undercuts Defendant's claims that all such warrants are per se unconstitutional "general" warrants that rifle through "billions" of innocent people's search histories without individualized suspicion. *But see Skinner*, 489 U.S. at 624 (upholding minimally intrusive drug testing and recognizing the showing of individualized suspicion is not a constitutional floor beyond which a search must be presumed unconstitutional). Defendant's general warrant analogy is factually untrue and legally inaccurate. Here, the judicially approved search warrant narrowly requested a database inquiry for devices that searched the victims' home address. Even if these results had not been anonymized (they were), this type of database query does not intrude into the contents of any user account.[8]

Contrary to Defendant's suggestion, that the search here began with an attempt to locate the people responsible for a crime rather than from individualized

[8] Both federal and state constitutional protections against unreasonable searches "are personal to the person asserting them." *People v. Curtis*, 959 P.2d 434, 436-37 (Colo. 2001). Thus, to the extent Defendant and amici claim the warrant here intruded on the privacy rights of other Google users (including the co-defendants), they lack standing to do so.

suspicion of Defendant himself does not transform this narrow intrusion into a "general warrant" or justify discarding the reasonableness analysis that is the foundation of constitutional search and seizure law. The general warrants and writs of assistance the Framers set to eliminate with the Fourth Amendment involved unlimited intrusions into colonists' homes in search of a crime to charge them with. By contrast, the warrant here started with a crime to be solved – the murder of five people – and proceeded to a narrow search for devices that would lead to the people responsible. This is not equivalent to a general warrant.

Further, the lack of individualized suspicion is not the per se prerequisite that Defendant and EFF suggest. To the contrary, the Supreme Court has repeatedly upheld the reasonableness of minimally invasive government intrusions in the total absence of any individualized suspicion. *See National Treasury Employees Union v. Von Raab,* 489 U.S. 656, 679 (1989); *Skinner*, 489 U.S. at 624; *see also Michigan Dep't of State Police v. Sitz,* 496 U.S. 444, 455 (1990) (upholding sobriety checkpoints conducted without any individualized suspicion where the intrusion was minimal compared to the important governmental interests it furthered). And those searches were conducted without a warrant, whereas law enforcement here obtained judicial approval for this limited address-only keyword

database query. That process alone better protects constitutional rights. *See Birchfield*, 579 U.S. at 469 ("Search warrants protect privacy in two main ways. First, they ensure a search is not carried out unless a neutral magistrate makes an independent determination that there is probable cause to believe that evidence will be found. Second, if the magistrate finds probable cause, the warrant limits the intrusion on privacy by specifying the scope of the search").

Consistent with the principles underlying the Fourth Amendment, the keyword search here minimally intruded into a third party database looking for a narrow set of information. It is a far cry from the general warrants imposed on colonists. The query did not invade the contents of emails or wide swathes of digital information like phone contents or CSLI. It did not reveal anything about Defendant's search history except how many times he'd affirmatively asked Google to pull up the victims' address before he burned it down. The narrow scope of this keyword warrant also compares favorably to cell tower dump warrants and geofence warrants that pull CSLI for all devices at a crime scene.[9] The warrant

[9] If not narrowly tailored to a narrow time (cell tower) or time and location (geofence), these types of warrants have the potential to capture CSLI from hundreds of unrelated devices. *See, e.g.*, Mason Kortz & Christopher Bavitz, *Cell Tower Dumps*, Boston B.J., Winter 2019, at 27; *United States v. Rhine*, No. CR21-0687 (RC), 2023 WL 372044, at *19 (D.D.C. Jan. 24, 2023) (most recent case addressing geofence warrants that recognized more than 5,000 unique devices were responsive to a geofence warrant regarding the January 6th attack on the capitol).

here instead minimally intruded into the handful of devices that asked Google for directions to an address before Defendant turned it into a crime scene.[10]

C. Address-only Google keyword warrants are constitutionally reasonable.

The present case highlights both the rare circumstances where a Google keyword search warrant is necessary and the constitutional reasonableness of that procedure in the address-only context. Facing an otherwise unsolvable multiple homicide, a judicially approved warrant allowed a narrow query to a Google database that openly logs the web activities of its users and provides them with alternative tools for using Google services without exposing such information.

The balance of interests is not close. The need to solve the murder of fellow citizens is a crucial need that outweighs the minimally private information disclosed through this address-only database inquiry. Even in its broadest conception, the governmental minimally intruded into an area of questionable privacy interests to ultimately provide shallow information that is categorically

[10] *Carpenter* expressly declined to address cell tower warrants and courts nationally have largely found no reasonable expectation of privacy in such data. *See Cell Tower Dumps*, *supra* n.9. As to geofence warrants, the recent *Rhine* decision comprehensively reviewed the law and upheld a carefully drawn geofence warrant that produced anonymized device information in a multi-step process that minimized the deanonymized information the government received. *See Rhine*, 2023 WL 372044, at **21-32.

distinct from CSLI or sensitive personal information. In other words, warrants seeking nothing more than users' affirmative searches for the address of a crime is a small cost to our collective privacy interests that cannot override society's interest in identifying those who murder our fellow citizens.

Thus, to the extent this Court is looking to create a rule for future cases, it should hold that address-only keyword warrants, like the one here (supported by probable cause and sufficiently particular), are constitutionally reasonable.

D. "Expressive" content searches are adequately addressed by the *Tattered Cover* balancing test.

In arguing for the reversal of the trial court's suppression ruling, EFF and EPIC focus almost exclusively on potential misuses of keyword warrants to broadly obtain information about peoples' personal, political, or medical information and raise particular concerns about law enforcement hunting those seeking abortion care. These concerns are misplaced, not only because of their irrelevance to the warrant at issue, but because Colorado has already staked a clear path for warrants touching on expressive rights. *See Tattered Cover*, 44 P.3d at 1056 (holding the Colorado Constitution requires a more substantial justification for law enforcement searches of bookstore records because they implicated the expressive rights of bookstores and their customers).

In *Tattered Cover*, this Court recognized the need for a more robust balancing test in those rare instances where search warrants seek expressive materials or otherwise implicate citizens' expressive rights; such as in that case, customer purchase records regarding "how to" books about manufacturing methamphetamine that were found inside a meth lab. *See id.* at 1056-59, 1061-63. Thus, where this intersection of search and expressive rights occurs, the government must demonstrate a sufficiently compelling need for the specific record sought. *See id.* at 1058. This balancing test requires courts to consider various factors including whether there are reasonable alternative means, the warrant's breadth, and the degree to which the government's action will generally chill the exercise of expressive rights. *See id.* at 1059. In so holding, this Court recognized the harms to expressive rights "will likely be minimal if the law enforcement officials' reason for wanting the book purchase records are entirely unrelated to the contents of the books," including, for example, if seeking to disprove an alibi or identify a suspect who left an unrelated book at a crime scene. *See id.* This expressive, content-based concern is consistent with First Amendment principles that apply strict scrutiny to regulations that target speech "based on its

communicative content" – that is the idea or message expressed. *See City of Austin, Texas v. Regan National Advertising of Austin, LLC*, 142 S.Ct. 1464, 1471 (2022).

This line between expressive and non-expressive information is why *Tattered Cover* already provides a workable standard for the various expressive, "what if" scenarios that are central to the amici briefs by EFF and EPIC.

Potential search engine keyword searches, like "how to build a meth lab" or "where can I get an abortion" are based on their communicative content. If law enforcement theoretically sought a Google keyword warrant for such terms, the *Tattered Cover* "compelling need" test would almost certainly apply because the need for such information is based on the expressive contents of those searches and raises the "general fear of the public" and "chilling effect" concerns underlying that heightened balancing test. *See Tattered Cover*, 44 P.3d at 1059-60.[11] By contrast, the address-only searches or address plus victim name searches that have

[11] One hypothetical EFF raises, an address-only keyword search for an abortion clinic, may or may not constitute expressive/communicative content subject to *Tattered Cover*. Unlike a residential address, there is the potential to sweep up sensitive information about citizens seeking healthcare. Critically, however, that does not make it *per se* expressive if, for example, law enforcement is searching for a person who bombed an abortion clinic, and the warrant was narrowly tailored to that purpose. Whether that would make *Tattered Cover* inapplicable or would instead be a case of the minimal constitutional harm that can be outweighed by the government's compelling need is a question best left for a future case.

been the subject of nearly every Google keyword warrant ever reported do not.[12] Knowing that your search for a particular address could be turned over to the government if that address is associated with a serious crime will not create a "general fear of the public" that would chill the public's willingness to use search engines or to seek expressive or communicative material.

If and when our judges are faced with keyword search warrants requesting expressive information, this Court's existing test and procedure from *Tattered Cover* can be applied. Accordingly, this Court should not countenance the alarmist hypotheticals that the EFF and EPIC amici brief present about potential abuses of keyword warrants or their theoretical use by out-of-state actors to broadly hunt for people searching controversial terms (like abortion care) to then contrive some type of crime they could have committed. Even putting aside that these hypotheticals effectively ignore the probable cause and particularity requirements that make such "what if" scenarios fanciful; Colorado law already ensures its citizens' protection where law enforcement warrants implicate expressive content.

[12] Andrea O'Sullivan, *The Government's Secret 'Google Search' Warrant Trap,* REASON (Oct. 12, 2021) (recounting the "rare" nature of keyword warrants and that they almost exclusively seek address-only or address plus victim name information). Available at: https://reason.com/2021/10/12/the-governments-secret-google-search-warrant-trap/

Thus, the expressive content search concerns raised by EFF and EPIC say nothing about the issue before this Court and offer little about the realistic future applications of Google keyword search warrants in Colorado.

CONCLUSION

CDAC respectfully asks this Court to affirm the district court's order.

Respectfully submitted.

Thomas R. Raynes
Executive Director
Colorado District Attorneys' Council

/s/Kevin E. McReynolds
KEVIN E. MCREYNOLDS, 40978*
Senior Appellate Deputy District Attorney
*Counsel for Amicus Curiae, the Colorado District Attorneys' Council

CERTIFICATE OF SERVICE

This is to certify that I have duly served this **AMICUS BRIEF SUBMITTED BY THE COLORADO DISTRICT ATTORNEYS' COUNCIL** on March 7, 2023 via Colorado Courts E-Filing System (CCES) upon all counsel of record.

/s/Kevin E. McReynolds