SUPREME COURT, STATE OF COLORADO 2 East 14th Avenue, Denver, CO 80203	
Denver District Court, Div. 5A Honorable Judge Egelhoff Case Number 21CR20001	DATE FILED: March 28, 2023 9:32 PM FILING ID: 1F55255ADBE87 CASE NUMBER: 2023SA12
In Re: PEOPLE OF THE STATE OF COLORADO, Plaintiff, v. GAVIN SEYMOUR, Juvenile Defendant.	☐ COURT USE ONLY ☐
JENIFER STINSON (#35993) Alternate Defense Counsel Stinson Law Office 1245 E. Colfax Avenue, Suite 300 Denver, Colorado 80218 Phone: (303) 483-3161 E-mail: JStinsonLaw@gmail.com MICHAEL JUBA (#39542) Alternate Defense Counsel The Juba Law Office, PLLC 675 N. Grant Street Denver, CO 80203 Phone: (303) 974-1080 E-mail: Juba@JubaLawOffice.com MICHAEL W. PRICE (#22PHV6967) National Association of Criminal Defense Lawyers 1660 L Street NW, 12th Floor Washington, DC 20036 Phone: (202) 465-7615 E-mail: MPrice@NACDL.org	Case Number: 23SA12

REPLY BRIEF

CERTIFICATE OF COMPLIANCE

I hereby certify that this brief does not comply with all requirements of C.A.R. 28 or C.A.R. 28.1, and does comply with C.A.R. 32, including all formatting requirements set forth in these rules. Specifically, the undersigned certifies that:

The brief does not comply with the applicable word limits set forth in C.A.R. 28(g) or C.A.R. 28.1(g).

☒It contains 7,895 words (principal brief does not exceed 9,500 words; reply brief does not exceed 5,700 words).

I acknowledge that my brief may be stricken if it fails to comply with any of the requirements of C.A.R. 28 or 28.1, and C.A.R. 32.

Michael S. Juba, Atty Reg. #39542

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Constitutional Provisions

Secondary Sources

I. Introduction

Respondents and their two amici filed four briefs responding to Mr. Seymour's petition challenging the reverse keyword warrant. Their divergent responses only highlight the need for this Court's review. They mischaracterize the scope of the search and seizure, and they misconstrue the law in defense of a digital dragnet that the United States and Colorado Constitutions were designed to prohibit.

Respondents' briefs differ most obviously on whether this Court should apply heightened scrutiny under *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044 (Colo. 2002) and Article II, Section 10 of the Colorado Constitution, so Mr. Seymour elaborates on his position here. But Mr. Seymour maintains that under *Tattered Cover*, the Fourth Amendment to the United States Constitution, and Article II, Section 7 of the Colorado Constitution, the keyword warrant here was unconstitutional and that its evidentiary fruits should be suppressed.

II. *Tattered Cover* Applies & Was Not Satisfied

Under the United States and Colorado Constitutions, protected "expressive activities" include the right to receive information and ideas anonymously. When a search warrant intrudes on this activity, two things happen: first, the warrant must follow the Fourth Amendment's requirements with "scrupulous exactitude." *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978); *Stanford v. Texas*, 379 U.S.

476, 485 (1965); *Tattered Cover*, 44 P.3d at 1055. Second, following this Court's decision in *Tattered Cover*, the Colorado Constitution requires law enforcement to make an additional, "heightened showing," 44 P.3d at 1056, that there is "a compelling need *for the precise and specific information sought*," *id.* at 1058, which outweighs the "harm caused to constitutional interests by execution of the search warrant." *Id.* at 1059. As this Court explained, "[t]his heightened standard is necessary because governmental action that burdens the exercise of First Amendment rights compromises the core principles of an open, democratic society." *Id.* at 1057.

Mr. Seymour maintains, as he has from the beginning, that *Tattered Cover* applies to the keyword warrant here and that the government failed to make this heightened showing. *See* Exhibit 1 (Motion to Suppress) at 11; Exhibit at 5 (Reply) at 6; Exhibit 10 (8/19/2022 Transcript) at 100-01; Petition for Rule to Show Cause Pursuant to C.A.R. 21 [hereinafter "Rule 21 Petition"] at 46-57. And should this Court agree, then under *Tattered Cover*, the warrant was "not enforceable and should not have issued." 44 P.3d at 1047. As a result, the appropriate remedy, at least for Mr. Seymour, is suppression. *Id.* at 1060 (identifying the exclusionary rule as a procedural protection that might be afforded the target of a search later deemed unconstitutional under *Tattered Cover*); *see also* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. Rev. 112, 163-64 (2007)

("[I]f the government seeks to introduce improperly gathered information in a criminal trial, the First Amendment should require that the evidence be excluded.").

A. *Tattered Cover* Applies

Respondents and one of their amici claim that the keyword warrant does not implicate either the First Amendment or *Tattered Cover* because the search for an address is "not the type of information associated with expressive activities." People's Response to Rule 21 Petition [hereinafter "People's Response"] at 10 (internal); *see also* District Court's Response to Order to Show Cause [hereinafter "Dist. Ct.'s Response"] at 63; Brief of Colorado District Attorneys' Council as Amicus Curiae Supporting Plaintiff-Respondent [hereinafter "C.D.A.C. Amicus Brief"] at 3. This is incorrect, as *Tattered Cover* itself makes clear—and as Respondent's other amicus, the Attorney General, apparently agrees. *See* Brief of Colorado Attorney General as Amicus Curiae Supporting Plaintiff-Respondent [hereinafter "A.G. Amicus Brief"] at 3-6.

The First Amendment and Article II, Section 10 of the Colorado Constitution safeguard "more than simply the right to speak freely." *Tattered Cover,* 44 P.3d at 1051. They also guarantee the "right to receive information and ideas" anonymously. *Id*. Indeed, "[w]ithout the right to receive information and ideas, the protection of speech under the United States and Colorado Constitutions would be

meaningless." *Id.* at 1052. A bookstore is one place "where a citizen can explore ideas, receive information, and discover myriad perspectives on every topic imaginable." *Id.* Today, Google serves a similar function.

Like the bookstore in *Tattered Cover*, people use Google to navigate the vast amount of information on the internet. *See* A.G. Amicus Brief at 5. Sometimes the information they seek may be mundane. Sometimes it may be highly personal. *See* Brief of Electronic Frontier Foundation as Amicus Curiae Supporting Defendant-Petitioner [hereinafter "E.F.F. Amicus Brief"] at 6-7; Brief of Electronic Privacy Information Center as Amicus Curiae Supporting Defendant-Petitioner [hereinafter "E.P.I.C. Amicus Brief"] at 6-8. Sometimes it may be offensive. And sometimes it might even relate to potential criminal activity, like the "how to" books in *Tattered Cover* that offered instructions on creating a secret drug lab.[1] Depending on one's perspective, the search for an address could be any combination of these. It can be hard to tell, and people may have any number of reasons for searching an address.[2]

[1] There are also currently 7,900,000 results on Google for "how to manufacture amphetamine." *See* https://www.google.com/search?q=how+to+manufacture+amphetamine (last visited Mar. 23, 2023).

[2] In fact, the warrant led the government to seize the records of 61 searches, many of which were conducted outside of Colorado, and one of which belonged to E.M., who investigators only cleared of involvement after obtaining a warrant to search the rest of their Google account. See Rule 21 at 44.

The First Amendment, however, does not discriminate based on the content of the query or the nature of the information sought. It does not privilege some inquiries over others, and for good reason. *See* A.G. Amicus Brief at 3 ("If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch.") (quoting *Stanley v. Georgia*, 394 U.S. 557, 565 (1969)). Indeed, the very purpose of the First Amendment was to prevent the suppression of "unpopular" ideas "at the hand of an intolerant society."[3] *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995); *see also Texas v. Johnson*, 491 U.S. 397, 414 (1989) ("If there is a bedrock principle underlying the First Amendment, it is that the government may not prohibit the expression of an idea simply because society finds the idea itself offensive or disagreeable."). This Court should therefore find that Google search queries, including searches for a residential address, are "expressive activities" under the First Amendment and that *Tattered Cover* applies to the keyword warrant here.

[3] Thus, an "address-only" exception for keyword warrants, as amicus CADC proposes, would be both undesirable and unconstitutional. *See* C.D.A.C. Amicus Brief at 17-18.

B. *Tattered Cover* Was Not Satisfied

1. There Was No "Compelling Need"

Tattered Cover first requires the government to make a heightened showing, prior to the execution of a search warrant, that there is a "compelling need" for the information sought. 44 P.3d at 1058. Respondents and both of their amici assert that law enforcement met this burden, *see* People's Response at 18, Dist. Ct.'s Response at 64; A.G. Amicus Brief at 6; at 20-21, but the first time the People appear to have addressed it was in response to Mr. Seymour's motion to suppress. As a result, this case reaches the Court in the very procedural posture that *Tattered Cover* aimed to avoid by requiring an adversarial proceeding prior to a warrant's execution.[4] Moreover, on the merits, the warrant still fails to demonstrate a "compelling need" for two reasons: (1) it is overbroad; and (2) there were "reasonable alternative means" of investigation to satisfy the government's asserted need.

Because "law enforcement officials' need to investigate crime will almost invariably be a compelling one" in the ordinary sense of the word, *Tattered Cover* requires courts to "engage in a more specific inquiry" to determine if there is a

[4] Although Google did not move to quash the third keyword warrant, Google did refuse to comply with the first two, which sought additional user records. The use of progressively narrower requests, as in *Tattered Cover*, likewise indicates that such a pre-execution hearing is necessary to protect innocent Google users. *See Tattered Cover*, 44 P.3d at 1060.

"compelling need *for the precise and specific information sought*." *Id.* at 1058 (emphasis original). Thus, "[f]or any particular expressive material sought, if the request is overly broad, then the law enforcement officials will not have a compelling need for that particular item." *Id.* at 1059. And as Mr. Seymour has argued at length, *see* Exhibit 1 at 19-21; Exhibit 5 at 6-9; Exhibit 7 (Defendant's Response to People's Written Arguments) at 4-5; Exhibit 10 at 14, 59; Rule 21 Petition at 73-83, the keyword warrant here was an overbroad digital dragnet unsupported by probable cause to search the data belonging to even a single Google user, let alone billions of them. *See also infra*, Section IV.

Second, because there were reasonable alternate ways of conducting this investigation that did not involve a reverse keyword warrant, law enforcement's need for the information sought cannot be "compelling." *Tattered Cover*, P.3d at 1059. The stated need for users' search data was to identify a suspect, as in *Tattered Cover*. *See id.* at 1062. But the record shows that law enforcement had at least two other reasonable options available to meet that need.

First, the three suspects captured on surveillance video all wore the same distinctive masks. Law enforcement could have canvassed the handful of local stores that sell these masks and inquired about recent purchases for three of them. *See* Exhibit 22 (Apple Search Warrant Affidavit) at 11 ("Your AFFIANT completed a Google search for Party City and observed that they sell masks that

appear to be similar to the mask worn by the three suspects"). And in fact, the police did eventually obtain such a receipt from Party City as well as additional surveillance video from the parking lot that might have identified the suspects or produced new leads earlier in the investigation. *See, e.g.*, Exhibit 23 (Exposition Dr. Search Warrant Affidavit) at 8 ("Detective BAKER was able to locate a purchase for three black masks which were purchased on August 4, 2020 at 6:15 p.m. from this store.").

Likewise, investigators knew that gasoline was used in the arson and that surveillance video showed one suspect with what appeared to be a gas can. *See* Exhibit 23 at 5. They also had a description of the suspects' vehicle. On August 13, 2020, an ATF agent canvassed several gas stations for "purchases of gasoline dispensed into gasoline cans or containers other than vehicles on the evening of 8/4/20 and early morning of 8/5/20." *See* Exhibit 24 (A.T.F. Report). However, this was the only time law enforcement canvassed any gas stations. And, the A.T.F agent tasked with the canvass only contacted six gas stations, all of which were on Tower Road and Chambers Road. Had investigators looked further afield and not narrowed the search to one road, they would likely have found surveillance footage or purchase of other individuals filling up gas cans. In fact, on October 20, 2020, investigators eventually obtained a still frame from a surveillance camera at a Kum & Go gas station in Green Valley Ranch neighborhood (the same neighborhood

where the fire occurred) that contained what law enforcement believed to be the same vehicle captured on neighborhood surveillance near the fire. *See* Exhibit 25 (Evidence Audit Trail).

As this Court explained, officials must exhaust such alternatives "before resorting to techniques that implicate fundamental expressive rights." *Tattered Cover*, 44 P.3d at 1059. While there was immense public and political pressure to solve this case, the investigation was fewer than two months old when law enforcement resorted to the keyword warrant. But the government still had reasonable alternatives, and there is no indication that searching through every Google users' account was the only way to identify the suspects in this case so early in the investigation.

2. The Warrant Substantially Chills First Amendment Activities

The People's failure to demonstrate a "compelling need" should be fatal to the warrant here; but even if it is not, the government's interest in identifying suspects does not outweigh the magnitude of the chill to First Amendment activities. *Tattered Cover* requires balancing the government's stated need against the "harm caused to constitutional interests by execution of the search warrant." *Id.* at 1059. Here, although it is difficult to calculate the extent of the harm, the chilling effect on search activity is likely to be far more substantial than the chill resulting from the search of a single bookstore. The basic nature of the harm is the same: causing

a general fear that negative consequences may follow if the government discovers which books invidivuals read, or which terms they searched. *See id.* at 1059. The difference is the scale, with a keyword warrant chilling the activities of billions of monthly Google users. *See* Rule 21 Petition at 85.

This does not necessarily mean that people will stop using Google, but empirical studies demonstrate that government surveillance does change people's search behavior. *See, e.g.*, Alex Matthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior*, MIT Sloane Working Paper No. 14380 at 4 (2017) (finding that Google searches for terms deemed personally-sensitive and government-sensitive were most negatively affected by the 2013 revelations concerning NSA surveillance programs);[5] Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 Berkeley Tech. L.J. 117, 124 (2016) (finding a decrease in traffic to Wikipedia articles on privacy-sensitive topics following the same 2013 revelations). Thus, the precedent this warrant sets has the potential to deter billions of people from searching for sensitive things, whatever they may be. *See, e.g.*, E.P.I.C. Amicus Brief at 10-11 (describing how keyword warrants will have a chilling effect on access to health information online).

The People simply fail to address this half of the balancing test, maintaining that it did not involve the type of "expressive ideas" that would raise First

[5] *Available at* https://ssrn.com/abstract=2412564.

Amendment concerns. People's Response at 27. The District Court addresses it for the first time, stating that the chilling effect was "minimal" under the circumstances because the information sought was "unrelated to the content or ideas" of the search. Dist. Ct.'s Response at 67. Similarly, the Attorney General likened it to "learn[ing] who purchased a particular book about baseball found at the scene of the crime." A.G. Amicus Brief at 18. But this case does not involve a search about baseball. It involves a search for the address of the house that burned down. Like *Tattered Cover*, the core of the government's argument rests on the premise that anyone who searched for the address was likely responsible for the arson.[6] *See Tattered Cover*, 44 P.3d at 1063. This rationale is thus directly tied to the contents of the Google query. And "[t]his is precisely the reason that this search warrant is likely to have chilling effects" on the Google-using public. *Id.* at 1063.

III. Google Users Have a Fourth Amendment Interest in Their Search Queries

A. Possessory Interest

Respondents and their amici consistently misrepresent the information at issue here as belonging to Google or "Google's database." *See, e.g.*, People's Response

[6] If the contents of the search were unrelated to the investigation, then at the very least, some additional facts would be necessary to establish a sufficient "nexus" to the crime. *See Tattered Cover*, 44 P.3d at 1058.

at 13; Dist. Ct.'s Response at 24; A.G. Amicus Brief at 11; C.D.A.C. Amicus Brief at 7, 11, 17. It does not belong to Google. It belongs to the individual users who created it, billions of them. Mr. Seymour has thoroughly briefed this issue at every stage of this case, but none of the Respondents or their amici have even mentioned it or introduced evidence to the contrary. Thus, this Court should find that Respondents concede the point and hold that users have a possessory interest in their search records under the Fourth Amendment and Article II, Section 7 of the Colorado Constitution. *See* Rule 21 Petition at 59-68.

It is critical to recognize, however, that Respondents' mischaracterization of who owns the data has analytical implications beyond whether users have a Fourth Amendment interest in it. This sleight of hand obscures the true scope of the search, *see infra*, Section V, by transforming the search of billions of people's personal data into a mere "database query." People's Response at 13; Dist. Ct.'s Response at 30; C.D.A.C. Amicus Brief at 14. So, to be clear: the data at issue here—all of the "ones and zeroes," People's Response at 13—belong to individual users like Mr. Seymour, and that data is stored in their accounts, just like their Gmail, Google Docs, or Google Photos. *See* Rule 21 Petition at 59-68. The data does not belong to Google. A user's account contents are their own digital property; they are not Google's "business records" or just a part of "Google's database," *cf.* People's Response at 24, 44; C.D.A.C. Amicus Brief at 11. A search

of queries made by billions of Google users is a search of billions of people's digital papers and effects.

B. Reasonable Expectation of Privacy

Mr. Seymour, like all Google users, also had a reasonable expectation of privacy in his Google queries. The District Court agrees with Mr. Seymour on this point, Dist. Ct.'s Response at 21-23, as does the Attorney General. A.G. Amicus Brief at 11 ("The warrants at issue in this case authorized the police to acquire records in which individuals had a reasonable expectation of privacy"). The People, however, maintain that it is "unnecessary" to decide this "murky" question. People's Response at 21. And the C.D.A.C. claims that there is only a "minimal" privacy interest at stake. C.D.A.C. Amicus Brief at 16. Such discord amongst those responsible for enforcing the law only demonstrates the need for this Court to affirm that search queries are constitutionally protected. Indeed, it is troubling that it seems the primary reason why investigators obtained a warrant here was because Google required one. The privacy rights of Coloradans should not depend on corporate policies and this Court should leave no doubt that search queries are private.

Amicus C.D.A.C. is unpersuasive that Mr. Seymour's privacy interest is somehow diminished, all but ignoring this Court's decisions in *People v. Sporleder*, 666 P.2d 135, 140-41 (Colo. 1983) (en banc) (declining to apply the

third-party doctrine to phone records), and *Charnes v. DiGiacomo*, 612 P.2d 1117, 1121 (1980) (en banc) (declining to apply the third-party doctrine to bank records). Rather, because the records here are one's digital papers, an account search *is* like rifling through the files in a locked home safe, or as Mr. Seymour has analogized, like searching his digital safe deposit box. *See* Rule 21 Petition at 67. Moreover, one of the reasons why the U.S. Supreme Court required a warrant to search a cell phone incident to arrest was because it likely contains information such as search and browsing history. *See Riley v. California*, 573 U.S. 373, 395–96 (2014) ("An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD."); *contra* C.D.A.C. Amicus at 18.

IV. The Keyword Warrant Was a General Warrant

Respondents' failure to recognize the Fourth Amendment interests that users have in their search data leads to warped analyses of the scope of the initial search that occurred. Because Respondents portray the data as "Google's" and liken it to Google's "business records," People's Response at 24, they conclude that the search was like issuing a subpoena or asking a business to make a "database inquiry." *Id.* at 12; Exhibit 8 (11/16/2022 Transcript) at 20 (stating that the warrant requested "a database query submitted to the custodian of the database, which was

Google"); C.D.A.C. Amicus at 14. But because that data belongs to billions of individual users, who all have their own privacy interest in it, a search across billions of such records is literally a search of billions of individual Google accounts. The warrant failed to specify even one account to search, and it lacked probable cause to search any of them, let alone justify a search of such magnitude. As a result, it was a modern-day general warrant. See Rule 21 Petition at 69-73, 104.

The District Court retorts that the keyword warrant does not share the same characteristics as the general warrants reviled by the Founders. Dist. Ct.'s Response at 33. But as the Supreme Court has repeatedly recounted, one of the two types of general warrants that gave rise to the Fourth Amendment authorized the search and arrest of "all persons connected with the publication of a particular libel." *Marcus v. Search Warrants of Prop. at 104 E. Tenth St., Kansas City, Mo.*, 367 U.S. 717, 727 (1961); *accord. Stanford v. Texas*, 379 U.S. at 482–83. And perhaps no such warrant was more famous than the one in *Wilkes v. Wood*, which involved a search for the publishers of *North Briton No. 45*, an anonymous and allegedly libelous pamphlet. *See id*. Although the crime in *Wilkes* was clear, the warrant did not specify which homes to search or who to arrest and was thus a form of "general warrant." *See* Rule 21 Petition at 105 n.18.

Like the search for the publishers of *North Briton No. 45*, the keyword warrant identified information, the contents of which were directly related to the crime under investigation, and the possession of which was perceived as probative of the perpetrators' identity. While that information was undoubtedly different from the information here, the First Amendment still does not discriminate based on its perceived value to society. *See supra,* Section II(A). Had British officials searched the colonists' homes for anyone with directions to Griffin's Warf around the time of the Tea Party, the Founders would have likely had the same reaction. Mr. Seymour thus analogizes the *Wilkes* search of people's houses for physical papers to the keyword search here of people's online accounts for their digital data. *See* Rule 21 Petition at 80-81, 102 (likening the keyword warrant to the search of diaries in a billion-story apartment building).

The People take issue with this analogy because a *digital* general warrant does not require investigators to "visually" examine either the homes or the search history of billions of people. *See, e.g.,* People's Response at 12-14, 26, 35. The Fourth Amendment, however, covers more than just "visual" inspections. *See, e.g.*, *Klayman v. Obama*, 957 F.Supp.2d 1, 37 (D.D.C. 2013) (phone call records); *United States v. Jones*, 565 U.S. 400, 408-411 (2012) (GPS tracking); *People v. Unruh*, 713 P.2d 370, 378-79 (Colo. 1986) (dog sniffs). While an officer did not manually review the search history of billions of Google users, he did commandeer

Google to do it electronically, s*ee infra*, Section V, and the distinction is not reassuring. On the contrary, it is even more concerning because the search here was outsourced, automated, and unnoticeable to individual users at the time. *See Jones*, 565 U.S. at 420 (Alito, J., concurring) (reasoning that to achieve the effect of a GPS tracker without technology, it would have required an officer to have "secreted himself somewhere in a coach and remained there for a period of time," a feat which "would have required either a gigantic coach, a very tiny constable, or both—not to mention a constable with incredible fortitude and patience.").

Another way to understand whether "visual" examinations matter is to consider a hypothetical: a scenario where the government has the capability to scan the contents of every cell phone in the country, quickly and easily, for the presence of a given file, perhaps a PDF of *North Briton No. 45*. Even if the government could describe that file down to its last one or zero, searching every cell phone in the country for it would still be a search of every cell phone in the country. Indeed, searching even one phone for it would be a Fourth Amendment search. *See Riley*, 573 U.S. at 386; 397 (recognizing that "users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference"). In this situation, the constitutional analysis does not turn on what the file was or on how well the government described it. *See id.* at 395-96.

And there is no constitutional exception for searching everyone's phone (even for just one little thing).

Today, the contents of cell phones today may be indistinguishable from real-time backups stored in online accounts with companies like Google. As a result, there is little difference between private data stored on a physical device and the same data stored in an associated account in 'the cloud.' Consequently, the search of a billion Google accounts is not far removed from the search of a billion cell phones, data that the Supreme Court said can be even *more private* than the physical papers in a house. *See Riley*, 573 U.S. at 396-97. Mr. Seymour does not ask this Court to hold that all warrants for search queries are unconstitutional, but he does ask this Court to find that this warrant, to search all queries, is precisely the type of dragnet that the Fourth Amendment was designed to prohibit.

V. The Warrant Was Overbroad[7]

Respondents do not accept the fact that this warrant authorized the search of over a billion user accounts. *See* Exhibit 8 at 27 ("that's just not what the search warrant does"); Dist. Ct.'s Response at 73; People's Response at 35, 41. But this

[7] The District Court notes that Mr. Seymour's Petition did not include a standalone section on probable cause. Dist. Ct.'s Response at 36, fn.5. However, the determination of whether a search is overbroad is rooted in whether there is probable cause to support the requested search; so probable cause is a necessary component of the analysis needed to address overbreadth, which Mr. Seymour briefed extensively in his Petition.

conclusion should not be credited because the record does not support it. At the motions hearing in the trial court Google employee Nikki Adeli testified that: gathering the information sought by the search warrant included a search of all authenticated and unauthenticated users' search history; that the search was not limited by geography; that Google has a billion active monthly users; and that each day Google receives billions of searches. Exhibit 10 at 36-40. The prosecution conceded this claim, noting at the hearing "[y]es, there are billions of Google users." *Id*. at p. 41. Notably, the prosecution declined to cross examine the Google witness and offered no evidence or argument to contradict the evidence offered by Google. Thus, the record and evidence demonstrate without opposition that the keyword warrant resulted in the search of private data stored in billions of individual Google accounts.

The reason Respondents must disagree is that there was no probable cause to search billions of Google accounts. Indeed, there was no probable cause to search any particular account, and certainly not Mr. Seymour's. The warrant never once mentions his name. Instead, Respondents repeatedly note that the house was "not on a corner lot" and was thus likely a "targeted" and "personal" attack on the house and its occupants. People's Response at 2, 30; Dist. Ct.'s Response at 11, 29, 39. And as a result, they conclude, there was probable cause to believe that "the person or persons targeting the home sought its location and/or directions" and that

Google had those records. Dist. Ct.'s Response at 39; *see* People's Response at 31-32. But this does not amount to probable cause to search any one Google account. *See People v. Gutierrez*, 222 P.3d 925, 938 (Colo. 2009) ("probable cause must exist to invade each individual's constitutionally protected interests").[8] Likewise, it was not sufficient to searh more than one account. *See, e.g.*, *United States v. Chatrie*, 590 F. Supp. 3d 901, 925 (E.D. Va. 2022) (finding a "geofence" warrant unconstitutional for lack of particularized probable cause); *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979). And it was therefore not sufficient to search Mr. Seymour's account. *See Gutierrez*, 222 P.3d at 940.

As in *Gutierrez*, probable cause is required to intrude upon "each constitutionally protected privacy interest an individual may have," regardless of whether it involves a search of their person or their private documents. 222 P.3d at 937; *see also United States v. Jaramillo*, 25 F.3d 1146, 1151 (2d. Cir.1994) ("[A]ny invasion of a person's Fourth Amendment interests must be justified at least by 'specific and articulable facts' directed to the person whose interests are to be invaded." (quoting *Terry v. Ohio*, 392 U.S. 1, 21, 88 S.Ct. 1868, 20 L.Ed.2d 889 (1968)). Moreover, this principle "applies with equal or greater force when the search targets an individual's documents." *Gutierrez*, 222 P.3d at 938. Therefore, it

[8] Indeed, given how often people use Google for all aspects of their lives, Respondents' argument proves too much. It would apply to any crime where a location was "targeted," including every house burgled and every business robbed.

is not enough to establish probable cause that evidence will be located at Google headquarters or somewhere on their servers. *See id*. ("probable cause may not be analyzed merely in relation to the property or premises searched. Rather, unless the custodian or business itself is pervaded by fraud, probable cause must be analyzed in relation to each individual's constitutionally protected interests").

But perhaps equally important, the government's theory of probable cause does not make sense. If the house was "targeted," then it is logical to believe that the suspects knew the location of their target. If "the suspects wanted to get to this particular residence," it does not follow that they did not "know where it was or how to get there." People's Response at 31. Indeed, the warrant affidavit contradicts itself on this point, stating that, "Based on the information provided, YOUR AFFIANT believes that the suspects entered the home and *may have been familiar with the residence*." Exhibit 14 (Keyword Search Warrant) at 7 (emphasis added). If police believed that the suspects were "familiar" with the residence and "targeted" it, then it is hard to see why it would be "probable" that they did not know where it was.[9] Thus, this Court should find that the magistrate did not have a substantial basis for finding probable cause to search Mr. Seymour's account, let alone billions of accounts.

[9] Respondents offer no defense to Det. Sandoval's admission during testimony that he had nothing more than a "hunch" that the address "could have possibly been searched." *See* Rule 21 Petition at 77-78.

Respondents invite this Court to ignore the absence of probable cause for the scope of the initial search and focus instead on the "narrow" data to be seized. Dist. Ct.'s Response at 54; People's Response at 21; *see also* A.G. Amicus Brief at 12 ("this Court should examine the breadth of the *requested* records, not the ministerial steps Google would take to locate them"). They claim police did not need probable cause to search Mr. Seymour's account specifically, but just establish a fair probability that the perpetrator searched Google for Truckee St. People's Response at 35-38; Dist. Ct.'s Response at 48. But probable cause must be narrowly tailored as to both the items to be seized *and* the place to be searched. Thus, in *Gutierrez*, it was unconstitutional to search thousands of tax returns held by a tax preparation company even though investigators were "only" looking for mismatched taxpayer identification numbers. 222 P.3d at 930. Likewise here, the "place" to be searched was, in effect, more than a billion individual Google accounts. In such circumstances, this Court has been explicit: probable cause must by analyzed "in relation to each individual's constitutionally protected interests" and not "merely in relation to the property or permises searched"—*especially* when a search of digital "documents" is at issue. *Id.* at 938, 940. This Court should therefore decline to accept Respondents' invitation.[10]

[10] Adopting the Respondents' view would mean, by analogy, that there is no need for probable cause to search any one cell phone, so long as there is a fair probability of finding the files sought on *someone's* cell phone.

Finally, the Attorney General claims that this Court should not examine Google's "ministerial" actions in conducting the initial search because "it was not an official, governmental intrusion into the protected interests of any Google user whose record was not ultimately disclosed to the police." A.G. Amicus Brief at 12. Google, however, did not conduct this keyword search of its own volition or for its own business purposes. *See* Exhibit 10 at 64. The only reason Google did so here was because a signed warrant commanded them to do it. *Id.* And having commandeered Google with a warrant, the government cannot "circumvent[] the requirements of the fourth amendment by directing a third party to perform and search that would be improper if the police did it themselves." *People v. Pilkington*, 156 P.3d 477, 479 (Colo. 2007) (en banc), *quoting People v. Chastain*, 733 P.2d 1206, 1214 (Colo. 1987). The government initiated the action by compelling Google to search for the keyword terms, and Google conducted the search for the express purpose of complying with law enforcement's warrant. *See Pilkington*, 156 P.3d at 479; *United States v. Smythe*, 84 F.3d 1240, 1242-43 (10th Cir. 1996). Far from being incidental to the issue in the case, that massive search was the central action commanded by the warrant at the behest of the government and therefore constituted state action.

VI. The Warrant Was Not Particularized

Ordinarily, a warrant is required to search even a single Google account. And to obtain such a warrant, as the government often does, it is necessary to identify the account to be searched. *See, e.g.*, Exhibit 26 (Google Account Search Warrant Affidavit) at 1. That does not mean that police must identify an account by the owner's real name; it may be sufficient to provide a username or account number. But the warrant must still specifically identify the account to be searched. And ordinarily, a warrant missing such information would violate the Fourth Amendment's particularity requirement because it would not be clear which accounts police may search, inviting impermissible officer discretion. Yet that is what happened here, and Respondents would have this Court dispense with that requirement so long as police want to search billions of accounts at once.

Respondents counter that the keyword warrant sufficiently identified the accounts to be searched because it established "parameters." *See* People's Response at 25; Dist. Ct.'s Response at 52 ("Here, the *parameters* for the search established 'the place to be searched.'"). Those "parameters" were the "specified search terms during the specified timeframe." Dist. Ct.'s Response at 52. Once again, however, Respondents conflate the place to be searched with the things to be seized. These "parameters" applied to the data that Google was required to provide

to investigators—*i.e.*, the data seized. *See* People's Response at 25. They did not limit the scope of the initial search in any meaningful way.[11]

Moreover, even with respect to the data seized, these parameters were not clear or effective. Just five of the 61 queries were exact matches to the keywords in the warrant, with the rest containing "other words" or no terms at all. *See* Rule 21 Petition at 87-88. The People now adopt a tortured reading of the warrant to claim it was obvious they could seize records of queries containing additional words. But that is no defense, as such an open-ended approach only injects additional uncertainty over the records to be seized and invites "seizure of one thing under a warrant describing another." *Marron v. United States*, 275 U.S. 192, 196 (1927).

The parameters also did not attempt to limit the data seized by geography, which was evident in the two queries produced from Illinois and the 21 with no location given. *See* Rule 21 Petition at 41. And in practice, the parameters were not sufficient to prevent police from seizing data from people with no connection to the crime. One woman, E.M., who searched for the address and was later cleared, became the subject of an additional warrant seeking her entire Google location

[11] It is unclear whether Google was able to limit the number of accounts searched using the timeframe provided, as doing so would require them to already know which accounts had run queries during those weeks. That is the same reason Google cannot limit the geographic scope of the initial search. *See* Exhibit 10 at 40-41. Regardless, it is not a meaningful parameter if it still permits the search of billions of accounts.

history and search history. *See* Rule 21 Petition at 44. "Parameters" are no substitute for particularity.

Similarly, this Court should reject the People's analogy to court orders for the production of documents issued under C.R.S. § 16-3-301.1. Such orders concern the production of a company's own business records, not other people's private papers and effects. *See supra*, Section III. And as a result, they employ a lower standard than probable cause, requiring only that the records are in the "actual control or custody of a business entity." § 16-3-301.1(2) (2022). Thus, for example, such a court order would be insufficient to compel a bank to produce documents from a client's safe deposit box, or a hotel to produce a guest's diary from their room, or a self-storage company to produce tax returns from a customer's unit. Indeed, when Coloradans have an expectation of privacy in the information sought, such as bank or telephone reocrds, and the government seeks to compel production with a subpoena, officials must demonstrate probable cause exists for a search of those records, and criminal defendants must be afforded the opportunity to challenge the demand for them. *See People v. Mason*, 989 P.2d 757 (1999). Furthermore, probable cause in this context means a sufficient "nexus between the materials and the charges against the defendant," not just whether the information exists with a third-party business. *Id.* at 761.

Finally, the District Court complains that Mr. Seymour's particularity arguments are "overly technical." Dist. Ct.'s Response at 50-51; *see also id. at* 56. Mr. Seymour disagrees: If the content of a Google query is at issue, and the warrant revolves around nine delineated variations of the same street address, then seizing records with other keywords appended is not a hyper-technical problem. It is true that "[i]nnocent individuals' privacy rights are often implicated in the execution of search warrants," as in the physical search of a house with multiple residents. Dist. Ct.'s Response at 57. But even if police need not use a "scalpel," *id.*, the Supreme Court still requires "scrupulous exactitude" for searches implicating expressive activities, including the anonymous receipt of information and ideas. *See supra*, Section II. Here, at very least, that would seem to demand police identify the accounts to be searched with the same degree of particularity required for searching one.

VII. The Good Faith Exception Does Not Apply

The good faith exception does not apply in this case. As Justice Holmes observed:

> "Anyone who respects the spirit as well as the letter of the Fourth Amendment would be loath to believe that Congress intended to authorize one of its subordinate agencies to sweep all our traditions into the fire, and to direct fishing expeditions into private papers on the possibility that they may disclose evidence of crime… It is contrary to the first principles of justice to allow a search through all respondents' records, relevant or irrelevant,

> in the hope that something will turn up." *FTC v. Am. Tobacco Co.*, 264 U.S. 298, 305-06 (1924).

"It is true that in an ideal system an unreasonable request for a warrant would be harmless, because no judge would approve it. But ours is not an ideal system, and it is possible that a magistrate, working under docket pressure, will fail to perform as a magistrate should." *Malley v. Briggs*, 475 U.S. 335, 345 (1986). The good faith test "imposes upon the officers involved in obtaining and executing a search warrant a continuing duty to exercise reasonable professional judgment. An officer may not automatically assume that a warrant is valid because a reviewing magistrate has executed it." *People v. Randolph*, 4 P.3d 477, 483 (Colo. 2000). The police in this case performed an exhaustive investigation and detailed their findings in an affidavit, which produced a warrant. The existence of an extensive investigation and the production of a warrant do not establish good faith. The affidavit omitted relevant and material facts, failed to establish with specificity the place to be searched, and failed to establish the necessary nexus between the crime itself and the place to be searched. "'By definition, in *every* case in which the prosecution seeks the benefit of *Leon*, a magistrate has issued a warrant… Because issuance of a warrant is a constant factor in these cases, it cannot logically serve to distinguish among them.'" *People v. Gutierrez*, 222 P.3d 925, 942 (Colo. 2009) (citation omitted). "An affidavit that provides the details of the investigation,

yet fails to establish a minimal nexus between the criminal activity described and the place to be searched, is nevertheless bare-bones." *Id*. at 941.

Omission of relevant and material information qualifies as a "false statement" for purposes of the good faith analysis. In *People v. Kazmierski*, 25 P.3d 1207, 1214 (Colo. 2001), the Court analyzed the first prong of the good faith test based on whether an affidavit was "misleading because it omitted" certain information. *Id.* (citing *People v. Winden*, 689 P.2d 578, 583 (Colo. 1984)). The nature and scope of this search were pieces of information recklessly omitted. The difficulty of conceptualizing what a reverse keyword search actually entails highlights the relevance and materiality of this information. The affidavit describes the requested information to be produced, but does not detail the process of obtaining the information at all. An apt analogy would be if a search warrant affidavit requested the production of only cell phone users who stored child pornography on their phones, but failed to mention that the police would need to search every cell phone in the country to produce this information. The omission of the relevant and material facts of what was to be searched and how the search was to be performed qualifies as knowing or reckless falsehoods for purposes of the good faith analysis.

The third and fourth prongs of the *Leon* test also fail to establish the officers acted in good faith. There is a failure to establish with specificity the place to be searched and also the nexus between the crime that occurred and the place to be

searched. The linchpin in this analysis is the failure to identify Mr. Seymour's account as one to be searched at all. A warrant cannot contain the required specificity detailing the place to be searched if the officers do not or cannot know what they are searching until after the search occurs. Nor can the required nexus be present if the object of the search is never identified.

It is well-established that an affidavit will fail the good faith analysis if it cannot establish "a nexus between the alleged illegal activity" and the place to be searched. *People v. Leftwich*, 869 P.2d 1260, 1268 (Colo. 1994). *See also People v. Altman*, 960 P.2d 1164, 1170-71 (Colo. 1998) (holding that affidavit will fail good faith analysis if it contains "wholly conclusory statements" or fails to connect "the evidence to the place to be searched."). And once again, this Court's decision in *Gutierrez* is highly instructive. *See* 222 P.3d at 928-29. In holding that the police lacked good faith to search all tax records held by the tax preparation company, the *Gutierrez* court stated:

> "The supporting affidavit in the present case does not merely fail to establish a 'sufficient nexus' between Gutierrez's tax return and the suspected criminal activity, it fails to establish any connection at all between Gutierrez and criminal activity… The affidavit makes no direct mention of Gutierrez, his client file, or his tax return, and there is no ancillary evidence which could link Gutierrez himself to the suspected criminal conduct. The most that can be objectively inferred from the affidavit is that Trejo's file contained false SSN information and that some unknown number of other clients may have, at some unknown point in the past, provided similarly false information. Such a warrant is so lacking in probable cause to believe that evidence of a crime will

> be found in Gutierrez's file that no reasonably well-trained officer could rely upon it.
>
> …
>
> The fact that, of the 5,000 files searched and seized only 1,300 were found to contain evidence of wrongdoing, highlights the absence of any nexus between the particular tax returns searched and criminal activity. It is difficult to understand how reasonably well-trained officers searching through 5,000 different individuals' client files, the substantial majority of which were free from any evidence of wrongdoing, would not, on some basic level, be aware that their endeavor was essentially a fishing expedition." *Id*. at 943-44.

The Detectives in this case admitted that prior to the keyword search warrant there was no suspicion at all that Mr. Seymour's Google account would hold the information the police sought. The affidavit failed to establish the sufficient nexus between Mr. Seymour's Google account and the criminal activity. The affidavit makes no mention of Mr. Seymour, his Google account, his search history, and there is no ancillary evidence which could link Mr. Seymour himself to the suspected criminal conduct. The suggestion that somebody may have searched for this address, because the house was not on the corner, is speculative at best. The initial part of this investigation focused on the immediate family members of the household, because the Detective initially concluded that it must have been somebody who knew this family who started the fire. Only after these initial search warrants failed to produce any suspects did the Detective claim that the opposite was actually self-evident: it must have been a stranger who set the fire. And the stranger must have searched for the address. And he must have used his Google

account to do so. These conclusory statements are not tied to any factual information, and certainly don't reference any connection to Mr. Seymour's account in the affidavit.

Such a warrant is so lacking in probable cause to believe that evidence of a crime will be found in Mr. Seymour's Google account that no reasonably well-trained officer could rely upon it. The fact that of the billions of accounts that had to be searched, only a handful were found to be responsive to the request, highlights the absence of any nexus between the particular accounts searched and criminal activity. This search is the equivalent of a digital fishing expedition, which squarely falls outside of the application of the good faith exception.

VIII. Conclusion

For the foregoing reasons, this Court should find that the reverse keyword warrant was unconstitutional under *Tattered Cover* and Art. 2, Section 10 of the Colorado Constitution, as well as the Fourth Amendment to the United States Constitution and Art. 2, Section 7 of the Colorado Constitution, and suppress all evidence and fruits obtained as a result thereof.

Dated this day: March 28, 2023

/s/ Jenifer Stinson

Attorney: Jenifer Stinson, #35993

Attorney: Michael S. Juba, #39542

Attorney: Michael W. Price, #22PHV6967

CERTIFICATE OF SERVICE
Parties: IN RE: PEOPLE OF THE STATE OF COLORADO
v. GAVIN SEYMOUR

I hereby certify that on March 28, 2023, a true and correct copy of this Motion was served upon all counsel of record through E-Filing.

Attorney: Michael S. Juba, #39542