DATE FILED: March 7, 2023 2:15 PM
FILING ID: B55D3103C1405
CASE NUMBER: 2023SA12

SUPREME COURT
STATE OF COLORADO
2 East 14th Avenue
Denver, Colorado 80203

Original Proceeding,
District Court, Denver County,
2021CR20001

In Re:

Plaintiff:
People of the State of Colorado,

v.

Defendant:
Gavin Seymour,

▲ **COURT USE ONLY** ▲

NATALIE HANLON LEH, Chief Deputy Attorney General

TRINA K. KISSEL, Senior Assistant Attorney General, #47194
PETER G. BAUMANN, Assistant Attorney General, #51620*
Ralph L. Carr Colorado Judicial Center
1300 Broadway, 6th Floor
Denver, CO 80203
Telephone: 720.508.6152
FAX: 720.508.6041
E-Mail: Trina.Kissel@coag.gov
Peter.Baumann@coag.gov
**Counsel of Record for Denver District Court*

Case No. 2023SA12

THE DISTRICT COURT'S
RESPONSE TO THE ORDER TO SHOW CAUSE

CERTIFICATE OF COMPLIANCE

I hereby certify that this brief complies with all requirements of C.A.R. 28(g) and C.A.R. 32, including all formatting requirements set forth in these rules. Specifically, the undersigned certifies that:

> The brief does not comply with C.A.R. 28(g) or C.A.R. 28.1 because it exceeds the word and/or page limit. A motion to accept the over-length brief has been filed contemporaneously with the brief.
>
> It contains 12,989 words.

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

s/ *Trina K. Kissel*
TRINA K. KISSEL, 47194*
Senior Assistant Attorney General

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

CASES

CONSTITUTIONS

STATUTES

RULES

STATEMENT OF THE ISSUE

Whether the magistrate judge had a substantial basis for issuing the reverse keyword search warrant that ultimately led to the identification and arrest of Gavin Seymour, and, if not, whether the evidence obtained under that warrant should be suppressed.

STATEMENT OF FACTS

I. An act of arson claims five lives, injures three others.

Early in the morning of August 5, 2020, police and firefighters responded to a fire at 5312 Truckee St., a residential address located in Denver's Green Valley Ranch neighborhood. Ex. 8 at 8; Ex. 16 at 3.[1] Upon arrival, these first responders saw at least one deceased victim located just inside the front door of the residence. Ex. 8 at 8. They soon learned that three other individuals had escaped through a second story window. *Id.* at 8–9. After more of the fire was contained, four other bodies were located inside the home. *Id.* at 9.

[1] All citations to Exhibits are to the Exhibits attached to the Petition.

II. Law enforcement identifies three suspects using a reverse keyword search warrant.

Law enforcement began investigating the source of the fire that same morning. Among other evidence, police obtained surveillance videos from other homes in the neighborhood. Ex. 8 at 9. From these videos, police could see that just before the fire started, three masked individuals "came to the side of the yard of the house that was on fire," and were "observed pointing towards the house, moving towards the house." *Id.* Shortly thereafter, these masked individuals were seen running "from the backyard area of the victim's home through the side yard" and out towards the street. Ex. 16 at 5. Two minutes later, the same camera began to pick up flames coming from home.

During their investigation, police determined that an accelerant had been used to start the fire, which began at the back of the home. Ex. 8 at 9–10. Police also took note of the neighborhood, specifically that the home was in a "rather populated subdivision," and that it "wasn't conspicuous," and was not located on a corner lot. *Id.* at 10.

As the investigation continued, law enforcement failed to identify a motive for the suspected arson, or any suspects. *Id.* Ultimately,

relying on the unique nature of the fire and the neighborhood in which it occurred, the police developed a theory that the home itself had been targeted. *Id.*

Based on this theory, law enforcement sought "to identify people that may have conducted internet searches pertaining" to the home located at 5312 Truckee or sought directions to that address. *Id.* at 11. To do so, the police drafted a list of nine variations of this address, and drafted a warrant to Google under which the internet provider would identify any user that searched for one of those nine variations in the two weeks leading up to the fire. Ex. 12.

Magistrate Judge Faragher approved the first iteration of this warrant. *Id.* But Google balked at the breadth of the request, which called for "records reflecting the personal identification of the subject account," including the full name of the account holder. *Id.* at 1. So, police drafted a new warrant, supported by a virtually identical affidavit, but this time asked for "anonymized information" relating to the users who ran these searches, as well as "all location data" for those users on August 4, 5, and 6, 2020. Ex. 14 at 1–2. Judge Faragher again

approved the warrant, but this time Google balked at the broad location data addendum. Ex. 14 at 9; Ex. 8 at 13.

This led the police to draft the warrant at issue. Ex. 16. This time, the warrant only requested "anonymized information," including IP addresses, for the accounts "found to have conducted any [of the nine identified] keyword searches." *Id.* at 1. The warrant indicated that if it became necessary to obtain further information "such as basic subscriber information," law enforcement would request that information "through appropriate legal process." *Id.* at 2. Based on the same affidavit attached to the prior warrants, a different Magistrate, Judge Zobel, approved the warrant. *Id.* at 9.

In response, Google produced a spreadsheet showing 61 responsive searches from five identifiable users. Ex. 17. Law enforcement then sought a second warrant for subscriber information for each of the five accounts. Ex. 18. Google responded and identified the accounts, including one belong to Gavin Seymour. Ex. 19.

From there, the police began issuing additional search warrants, including for cell phone records and social media accounts. Ex. 8 at 14.

Ultimately, Seymour was arrested and charged with five counts of first-degree murder, among other charges. Based on the District Court's understanding of the investigation, most of the other information obtained by law enforcement related to Seymour "flowed from" the reverse keyword search warrant "and was revealed from it." Ex. 8 at 18.

Seymour was sixteen years old at the time the crime was committed. Pet. ¶ 37.[2] Seymour was charged under Colorado's direct file statute, § 19-2.5-801(1)(a), C.R.S. (2020), and is being tried as an adult. Pet. at ¶ 36.

III. The District Court declines to suppress evidence obtained through the reverse keyword search warrant.

Last June, Seymour moved to suppress evidence from the reverse keyword search warrant. Ex. 1. After the motion was fully briefed, *see* Exs. 3, 5, the District Court held a hearing on August 19, 2022. Ex. 10 At the hearing, the District Court heard testimony from a

---

[2] There are two versions of the Petition. An 82-page version submitted at 9:15 AM on January 11, 2023, and a 108-page version submitted two hours later. The District Court cites to the later-filed Petition.

representative of Google and Detective Ernest Sandoval, the affiant who had applied for the warrant. *Id.*

The District Court entertained brief argument at the hearing, but at Defendant's request also solicited post-hearing briefing. Ex. 10 at 160. The parties filed briefs, Exs. 5, 6, and on November 16, 2022, the District Court denied the motions to suppress. Ex. 8.

The District Court concluded that Judge Zobel had a substantial basis for approving the reverse keyword search warrant. Ex. 8 at 26. The court began its analysis by observing that at every stage of their investigation, law enforcement had "resorted, in the first instance, to the legal process." *Id.* at 15. Returning to this theme throughout its ruling, the court noted that "what we have is the police doing exactly what we want the police to do . . . . If they need to conduct searches that implicate Fourth Amendment issues, go first to the courts to obtain authorization to do so." *Id.* at 16–17.

In concluding that Judge Zobel had a substantial basis to issue the warrant, the District Court rejected the argument that Seymour lacked a reasonable expectation of privacy in his Google search history. *Id.* at

21–22. And while it was unnecessary in light of its central ruling, the District Court also made factual findings relating to the good-faith exception to the exclusionary rule, finding that law enforcement had acted in good faith reliance on the warrant. *Id.* at 28–29.

SUMMARY OF ARGUMENT

In obtaining and executing this warrant, law enforcement acted exactly as they should. They sought judicial approval of the warrant, and even worked with the custodian of the records to address some of the custodian's concerns. And at each stage, the police relied on an affidavit to establish probable cause that satisfied two separate magistrate judges, and that the District Court called one of the more detailed and specific warrants it had ever seen.

The technology at issue here is novel. But the principles underlying application of the warrant requirement and exclusionary rule are not. On the deferential standard of review afforded the magistrate judge's probable cause determination, this Court should join the District Court in declining to suppress the evidence obtained as a result of the warrant.

And even if the Court disagrees as to the validity of the warrant, the good-faith exception to the exclusionary rule still precludes suppression. Because law enforcement acted exactly as they should, and in justifiable reliance on a judicial warrant, exclusion is not warranted.

ARGUMENT

I. The Court should dismiss the rule to show cause as improvidently granted.

Having issued the rule to show cause, the Court may still dismiss it as improvidently granted. *See People v. McGraine*, 679 P.2d 1084, 1085 (Colo. 1984) (noting that Court had previously discharged a rule to show cause as improvidently granted). Because Seymour has the same conventional appellate remedies available to any criminal defendant, the Court should discharge the Rule. *See* C.A.R. 21(a)(1).

An original proceeding pursuant to Art. VI, § 3 of the Colorado Constitution and Rule 21 is "an extraordinary remedy that is limited in both purpose and availability." *People v. Lucy*, 2020 CO 68, ¶ 11 (quotations omitted). Historically, there are "two basic requirements" for such proceedings: "First, the case must involve an extraordinary matter of public importance. Second, there must be no adequate

conventional appellate remedies." *People ex rel. Salazar v. Davidson*, 79 P.3d 1221, 1228 (Colo. 2003) (citations and quotations omitted). The Petition fails the second prong.

In recent years, the Court has framed these requirements disjunctively. *See, e.g.*, *People v. Hacke*, 2023 CO 6, ¶ 7. Even so, the Court's Rule 21 docket reflects an appreciation that its original jurisdiction should be cabined to "those extraordinary circumstances when no other adequate remedy is available." *Nelson v. Encompass PAHS Rehabilitation Hosp., LLC*, 2023 CO 1, ¶ 7 (citation omitted); *In re People ex rel. A.C.*, 2022 CO 49, ¶ 6.[3]

---

[3] In nearly all of the Court's recent Rule 21 matters arising on behalf of criminal defendants, the question presented could not have been raised on direct appeal. *See, e.g.*, *Hacke*, ¶ 9 (exercising original jurisdiction because defendant's "request for a preliminary hearing will be rendered moot after trial"); *In re People v. Cortes-Gonzalez*, 2022 CO 14, ¶ 23 (exercising original jurisdiction because "an order erroneously requiring disclosure of information protected by the attorney-client privilege . . . cannot be cured on direct appeal."); *In re People v. Greer*, 2022 CO 5, ¶ 17 (exercising original jurisdiction so that criminal defendant did not need to proceed to trial and appeal without counsel). *But see People v. Vigil*, 2021 CO 46, ¶ 14 (exercising original jurisdiction as to preliminary determination that, if allowed to stand, would "impact trial strategy and, potentially, decisions surrounding plea negotiations").

The Petition argues that no adequate appellate remedy exists because without Rule 21 review, "Mr. Seymour would have to forego a favorable plea offer, face a quintuple murder trial as a teenager, and risk being sentenced to life in prison." Pet. at ¶ 34. As sympathetic as Seymour's plight is, it is indistinguishable from that of any other criminal defendant whose effort to suppress evidence has been denied.

As the Petition notes, this Court held in 2012 that criminal defendants may not appeal an unsuccessful motion to suppress after entering a guilty plea. Pet. at ¶¶ 49–53 (citing *Neuhaus v. People*, 2012 CO 65, ¶ 16). There, this Court held that authorization for such "conditional pleas" "is better achieved by statute or court rule than by judicial decision." *Id.* ¶ 17. But in the intervening decade, neither this Court, nor the General Assembly, has established such a rule. As a result of this conscious inaction, Seymour is not unique among criminal defendants in having to weigh potential plea offers against proceeding to trial and raising the suppression issue on direct appeal.

Nor should Seymour's status as a juvenile alter the standard Rule 21 analysis. Section 19-2.5-801(1)(a), under which Seymour is being

tried as an adult in District Court, represents a legislative determination that he should be treated in virtually all respects as an adult for purposes of this criminal prosecution. Where the General Assembly has determined that juveniles tried in District Court should be treated differently—in the sentencing context—it has made that explicit. *See, e.g.*, § 18-1.3-401(4)(b)(I) (imposing separate sentencing requirements on juveniles convicted of class 1 felonies in district court).[4] It has not similarly elected to treat juveniles differently for the purposes of interlocutory appeal. *Cf. Mook v. Bd. of Cty. Comm'rs of Summit Cty.*, 2020 CO 12, ¶ 35 (interpreting legislature's decision to omit language from one statute that it included in another as intentional).

To be sure, Seymour faces difficult questions in litigating and potentially resolving this case. But those questions are no different than

---

[4] The U.S. Supreme Court cases holding that juveniles should be treated differently than adults also arise in the sentencing context. Pet. at 14. *See Roper v. Simmons*, 543 U.S. 551, 578–79 (2005) (eliminating death penalty for juvenile offenders); *Graham v. Florida*, 560 U.S. 48, 82 (2010) (eliminating life without parole sentences for non-homicide juvenile offenses); *Miller v. Alabama*, 567 U.S. 460, 489 (2012) (eliminating mandatory sentences of life-without-parole for juvenile offenders).

those faced by criminal defendants throughout the state. Those individuals routinely raise their appellate challenges on direct appeal. And so too should Seymour.

II. The reverse keyword search was a search subject to the U.S. and Colorado Constitutions.

A. Standard of review and preservation.

Before the District Court, the People argued that Seymour lacked a reasonable expectation of privacy in his Google search history. Ex. 10 at 108. The District Court rejected that argument Ex. 8 and 21–22. The District Court's factual findings on this point are afforded deference, but its legal conclusions are reviewed de novo. *People v. Tafoya*, 2021 CO 62, ¶ 23.

B. Seymour maintained a reasonable expectation of privacy in his Google search history.

1. Legal principles

Both the Colorado and U.S. Constitutions protect individuals "from unreasonable government searches and seizures." *People v. Davis*, 2019 CO 24, ¶ 15 & n.2 (citing U.S. Const. amend. IV; Colo. Const. art. II, § 7). For a "search" to fall within the ambit of these provisions, the

government's activity must violate "a subjective expectation of privacy that society recognizes as reasonable." *Tafoya*, ¶ 25 (quoting *Kyllo v. United States*, 533 U.S. 27, 33 (2001)); *see also People v. McKnight*, 2019 CO 36, ¶ 30 (observing that the question is the same under the Colorado Constitution).

"As a general matter, when a person voluntarily discloses information to a third party, even for a limited purpose, that person usually ceases to have a reasonable expectation of privacy in such information[.]" *People v. Gutierrez*, 222 P.3d 925, 935 (Colo. 2009). For example, under the Fourth Amendment, individuals generally do not maintain an expectation of privacy in financial records maintained by a financial institution, *United States v. Miller*, 425 U.S. 395, 443 (1976), the phone numbers they dial on their phones, *Smith v. Maryland*, 442 U.S. 735, 742 (1979), or garbage placed at the curb for pickup, *California v. Greenwood*, 486 U.S. 35, 39 (1988).

However, the U.S. Supreme Court has been hesitant apply the third-party doctrine to digital records. In *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018), the Court declined to extend the third-

party doctrine to cell-site location information, even though that data was maintained by a third party.

Moreover, this Court has "demonstrated a willingness to interpret the state constitution to afford broader protections than its federal counterpart." *McKnight*, ¶ 28. This is especially true as to the third-party doctrine. Splitting with *Miller* and *Smith* respectively, this Court has held that Coloradans maintain a reasonable expectation of privacy under the Colorado Constitution in their financial records, *Charnes v. DiGiacomo*, 612 P.2d 1117, 1120–21 (1980), and their telephone records, *People v. Sporleder*, 666 P.2d 135, 143–44 (Colo. 1983), even though both reside with third parties.

2. The records at issue here are categorically different than those available in a traditional third-party case.

Against this backdrop, the District Court rejected the People's argument that the third-party doctrine applied to Seymour's Google search history. Ex. 8 at 22 ("I'm not prepared to say that simply by availing oneself of the internet, that the users surrender all expectation of privacy with respect to that use."). Should the People renew this

challenge, this Court should similarly reject the conclusion that the third-party doctrine applies here.

In *Carpenter*, the U.S. Supreme Court declined to extend the third-party doctrine to cell-site location information in part because that information was "qualitatively different" than the records at issue in *Smith*, *Miller*, and the Court's other third-party cases. *Carpenter*, 138 S. Ct. 2216–17. Noting the "seismic shifts in digital technology" that enabled such cell-phone monitoring, the Court distinguished digital providers from the typical third-party lay witness. *Id.* at 2219 ("Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible.").

The same analysis applies here. Google's vast digital database is categorically different than the records at issue in *Smith* or *Miller*. With each passing day, the internet—and its infallible memory—becomes an even greater necessity in everyday life. When a person uses Google's search technology to identify an address or directions to that address they are not making a conscious choice to expose their whereabouts and

search history to a third party. That, alone, undermines application of the third-party doctrine.

Charnes is instructive. In splitting with the U.S. Supreme Court over financial records, this Court observed that "bank transactions are not completely voluntary because bank accounts are necessary to modern commercial life." *Charnes*, 612 P.2d at 1121 (citations omitted). Today, the same can be said for the internet in general, and Google search and Google maps in particular. The ubiquity of use and reliance on these tools, combined with their infallibility as a witness, undermines the justifications for the third-party doctrine.

Thus, as did the District Court, this Court should decline to hold that Seymour lacked a reasonable expectation of privacy in his internet search history.

III. The District Court correctly upheld the validity of the reverse keyword search warrant.

A. Standard of review and preservation.

This issue is preserved. Seymour challenged the search warrant's validity on state and federal constitutional grounds. Ex. 1, at 1, 11-23. When reviewing a suppression order, this Court defers to the trial

court's factual findings if the record supports them and reviews its legal conclusions de novo. *Tafoya*, ¶ 23.

B. The magistrate had a substantial basis for issuing the reverse keyword search warrant.

1. Legal principles

The Fourth Amendment to the U.S. Constitution requires that (1) all searches and seizures be reasonable; and (2) "a warrant may issue only if 'probable cause is properly established and the scope of the authorized search is set out with particularity.'" *People v. Smith*, 2022 CO 38, ¶ 26 (quoting *Kentucky v. King*, 563 U.S. 452, 459 (2011)); *see also* Colo. Const. art. 2, § 7; *Smith*, ¶ 26, n.2 ("Our state's Fourth Amendment counterpart also prohibits (1) unreasonable searches and seizures and (2) search warrants that either fail to establish probable cause or lack particularity."). A search conducted pursuant to a warrant is typically reasonable. *People v. Coke*, 2020 CO 28, ¶ 34.

"Probable cause exists when an affidavit for a search warrant alleges sufficient facts to warrant a person of reasonable caution to believe that contraband or evidence of criminal activity is located at the

place to be searched." *People v. Cooper*, 2016 CO 73, ¶ 9. This Court determines whether probable cause exists by examining the totality of the circumstances. *Id.* "[T]he central question for the reviewing court is not whether it would have found probable cause in the first place, but whether the magistrate had a substantial basis for issuing the search warrant." *People v. McKay*, 2021 CO 72, ¶ 10 (citation omitted). This Court presumes the warrant's affidavit is valid and confines its sufficiency review to the four corners of the affidavit. *Id.*

As to the particularity requirement, the warrant must describe "the place to be searched, and the persons or things to be seized." U.S. Const., amend. IV; *Pettigrew v. People*, 2022 CO 2, ¶ 52. A warrant is sufficiently particular where "it enables the executing officer to reasonably ascertain and identify the things authorized to be seized." *People v. Roccaforte*, 919 P.2d 799, 803 (Colo. 1996).

"[A]fter-the-fact scrutiny by courts of the sufficiency of an affidavit should not take the form of *de novo* review." *McKay*, 2021 CO 72 ¶ 10 (quoting *Illinois v. Gates*, 462 U.S. 213, 236 (1983)). "A grudging or negative attitude by reviewing courts toward warrants . . . is

inconsistent with the Fourth Amendment's strong preference for searches conducted pursuant to a warrant." *Gates*, 462 U.S. at 236 (citation omitted). This Court does not determine "whether it would have found probable cause in the first place, but whether the magistrate had a substantial basis for issuing the search warrant." *McKay*, 2021 CO 72 ¶ 10.

2. Background

The challenged search warrant sought court approval for Google to search for variations of the address where the fire occurred. Ex. 16 at 2. The warrant sought results limited to within 15 days prior to the crime's commission and contained several technical limitations. Ex. 16 at 2–3.

The warrant's affidavit, seven single-spaced pages long, described the crime and the investigation. It detailed video footage that officers recovered from neighbors, and discussed interviews with the surviving victims who did not know of anyone who would be targeting them. Ex. 16 at 5–7. It described that the fire started in the rear of the residence, and arson investigators concluded that gasoline, found on the living

room wall, was used as an accelerant. Ex. 16 at 8. It concluded by explaining why the affiant believed there was probable cause to search Google for responsive information:

> Based on the extreme nature of this crime and the extensive planning it must have taken to carry out the events involved in this offense, Your Affiant feels that this crime was very personal and involved a substantial amount of anger towards someone in the victim residence and/or was intended to send some sort of message. This belief is based on years of investigation of violent crimes and the motives associated with such crimes that Your Affiant has been exposed to over the years. Considering the personal nature of this offense, the actions of the suspects as observed on the surveillance videos, and the amount of planning that likely went into a coordinated attack such as this one, Your Affiant believes that there is a reasonable probability that one or more of the suspects searched for directions to the victim's address prior to the fire. The victim's home is in a densely populated subdivision and does not "stick out" as a house that would likely have been picked at random. It is not on a corner lot, which would be an easier target residence as there would be more area to move in before and after setting the fire. As such, it is reasonable to believe that this home was targeted, and that the person or persons targeting the home sought its location and/or directions in planning this attack.
>
> The information requested is limited to information that can be used to identify a person who engaged in a search for this residence close to but not after the offense occurred. No other contents of the account are being sought at this time. If this warrant yields an account that qualifies under the parameters set forth above, additional investigation will be

> conducted to determine if that person has any connection to this crime.

Ex. 16 at 8.

Judge Zobel approved the warrant. Ex. 16 at 13. Google executed it and produced anonymized information and IP addresses for five users. Ex. 4, ¶¶ 7, 15; Ex. 10 at 86. *See* Ex. 17. Through subsequent investigation and the execution of additional search warrants, law enforcement ultimately identified and charged three suspects, including Seymour.

Seymour moved to suppress the evidence obtained through the warrant, and the District Court denied the motion. Ex. 8. In an oral ruling lasting nearly ninety minutes, the District Court recited the factual background and general Fourth Amendment principles before addressing the warrant. The court determined that the search "was not a search of any individual user account" or "even a search for any specific content . . . [on] the internet." Ex. 8 at 19. Instead, it found that the warrant requested "a database query submitted to the custodian of the database, which was Google, which established certain search parameters." Ex. 8 at 20. The search warrant authorized, and law

enforcement received, "an anonymized list of IP addresses . . . that comported with the specific search parameters that were identified in the search warrant." Ex. 8 at 20.

Thus, the court concluded that despite the technology involved, the warrant was "subject to traditional review and analysis" under the Fourth Amendment. Ex. 8 at 23. In doing so, the court implicitly rejected the heightened standard of review from *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044 (Colo. 2002).

The court then conducted its Fourth Amendment analysis. First, it found the warrant wasn't overbroad: "although the warrant authorizes a search of this vast resource – what's being sought here is narrow. . . . deidentified or anonymized accounts of . . . this narrow group of users who searched for this particular address in this narrow time frame." Ex. 8 at 25. Accordingly, it concluded the warrant had "very precise particularity." Ex. 8 at 25.

As to probable cause, the court found the affidavit had "very specific factual assertions" about "why a particular keyword search of keywords being sought to be searched are relevant and are likely to

yield any included information with respect to it." Ex. 8 at 25. Specifically, the affidavit addressed "the nature of the neighborhood, the nature of the crime, [and] the likelihood that the address was being targeted," which led to "a likelihood that folks would use the internet to do that research and find those directions and such." Ex. 8 at 25–26. In fact, the court noted, "this particular affidavit and this particular search warrant is one of the more detailed and specific and narrowly tailored affidavits that this Court really has encountered in a long time." Ex. 8 at 26.

The court concluded that "the issuing magistrate had a substantial basis for finding that there was probable cause" and upheld the constitutionality of the warrant. Ex. 8 at 26.

3. Analysis

The trial court undertook a thorough analysis of probable cause, particularity, and overbreadth, which this Court should not overturn.

a. Reverse keyword searches are not per se unconstitutional.

First, Seymour argues the search warrant was a "general warrant" like those "reviled" by the Founders. Pet. at ¶¶ 146–51. The warrant here does not share those characteristics.

The Fourth Amendment prohibits "general warrants." *Thompson*, ¶ 18. "Historically, the general warrant . . . allowed police to arrest and search on mere suspicion that some illegal act had been committed." *People v. McCoy*, 870 P.2d 1231, 1238 (Colo. 1994) (Scott, J., concurring). General warrants gave the police "[the] broad authority to search and seize *unspecified* places or persons." *People v. King*, 16 P.3d 807, 813, n.6 (Colo. 2001) (emphasis added; citation omitted). They permitted "a general, exploratory rummaging in a person's belongings." *Coke*, ¶ 34.

"The principal evil of the general warrant was addressed by the Fourth Amendment's particularity requirement. . . ." *Ashcroft v. al-Kidd*, 563 U.S. 731, 742-43 (2011). The particularity requirement "ensure[s] that government searches are confined in scope to

particularly described evidence relating to a specific crime for which there is demonstrated probable cause." *Roccaforte*, 919 P.2d at 802 (citation omitted). The warrant's affidavit must therefore "supply a sufficient nexus between criminal activity, the things to be seized, and the place to be searched." *People v. Kerst*, 181 P.3d 1167, 1172 (Colo. 2008).

Seymour contends the District Court focused "on process—on the fact that police obtained a warrant—and did not address Mr. Seymour's argument that such general warrants are constitutionally impermissible." Pet. at ¶ 27. But "Fourth Amendment doctrines rooted in Colonial Era grievances do not always map neatly onto 21st century surveillance technologies." *In re Warrant Application for Use of Canvassing Cell-Site Simulator*, No. 22 M 00595, 2023 WL 1878636, at *21 (N.D. Ill. Feb. 1, 2023). The District Court applied traditional Fourth Amendment principles to the technology at hand, but it didn't just focus on the *fact* that a warrant was obtained. It considered whether the warrant satisfied the core Fourth Amendment requirements.

Seymour seems to be asking this Court to find reverse keyword warrant searches per se unconstitutional. Pet. at ¶ 18. The U.S. Supreme Court and this Court have rejected attempts to categorically invalidate types of searches. The validity of a search warrant "must be decided on the particular facts of each case." *Tattered Cover*, 44 P.3d at 1056. Even "presumptively protected materials are not necessarily immune from seizure under warrant for use at a criminal trial." *Zurcher v. Stanford Daily*, 436 U.S. 547, 567 (1978).

Seymour implies that courts have struck down geofence warrants as per se unconstitutional, Pet. at ¶ 18, but "no court has held that a geofence warrant is categorically unconstitutional." *Matter of Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 362 (N.D. Ill. 2020) (approving geofence warrant) ("*Arson*"); *United States v. Smith*, No. 3:21-CR-107-SA, 2023 WL 1930747, at *8 (N.D. Miss. Feb. 10, 2023) ("In essence, the Defendants' argument on this point seems to be a contention that geofence warrants in general violate the Fourth

Amendment. The Court declines to make such a sweeping determination.").

Thus, the District Court correctly focused on "process" here because process dictates the outcome.

b. The affidavit set forth probable cause to believe that evidence would be found in the place to be searched.

Seymour challenges the magistrate's finding of probable cause.[5] "[T]he Fourth Amendment requires no more" than the magistrate having a "substantial basis for concluding that a search would uncover evidence of wrongdoing." *Gates*, 462 U.S. at 236 (cleaned up). "Probable cause does not require certainty or even that it be more likely than not that a search will reveal evidence." *People v. Cox*, 2017 CO 8, ¶ 13. (cleaned up). Instead, there must be "a fair probability that items connected to a crime, whether they be contraband, instrumentalities, fruits, or even mere evidence of the crime, will be found at the time and

---

[5] Seymour's Petition does not have a standalone section on probable cause but challenges probable cause throughout his discussion of particularity and overbreadth. For ease of reference, this brief consolidates the probable cause arguments into one section.

place of a search." *People v. Coates*, 266 P.3d 397, 400 (Colo. 2011) (citation omitted).

By now, three judges have concluded there was probable cause—the two magistrate judges who authorized the three search warrants, and the District Court, which reviewed the third warrant for the motion to suppress.[6] The District Court remarked that "this particular affidavit . . . is one of the more detailed and specific and narrowly tailored affidavits that this Court really has encountered in a long time." Ex. 8 at 26.

Seymour refers to the first two warrants as "failed" warrants, but they are better characterized as "abandoned." Pet. at ¶ 154. A magistrate approved all three; only the third was executed and challenged. That Google, weighing its own interests, advocated for changes to the first two warrants but acquiesced to the third does not impact the Fourth Amendment analysis.

---

[6] Although the three search warrants included different parameters for timeframe and the data to be produced, the affidavits' explanations were similar as to why the detective believed evidence of the crime could be found at the place to be searched. Ex. 12, 14, 16.

Turning to the challenged warrant, the affidavit set forth that a crime was committed. Video footage showed three masked individuals lurking in the yard of the house just before a large fire erupted, killing five people. Ex. 16 at 5–6.

The affidavit then explained why the detective concluded the specific evidence sought would be found at the location to be searched, Google. Ex. 16 at 8–9. The crime would have taken "extensive planning," particularly as "a coordinated attack" among the three suspects seen on the video. Ex. 16 at 8. The affidavit refers to the suspects' actions captured on video: they appear together in the side yard, gesture at the back of the house, and apparently enter the back of the house to disperse the accelerant and light it on fire before fleeing on camera again though the side yard. Ex. 16 at 8.

The affidavit also explained why this particular house appeared to be the suspects' target. The "extreme nature" of the crime indicated someone in the house was targeted because, in the detective's experience, crimes like this usually have a personal motive—"a substantial amount of anger" at one of the victims or the intent "to send

. . . [a] message." Ex. 16 at 8. And the location of the house also suggested a targeted attack: "The victim's home is in a densely populated subdivision and does not 'stick out' as a house that would likely have been picked at random. It is not on a corner lot, which would be an easier target residence as there would be more area to move in before and after setting the fire." Ex. 16 at 8. Thus, "it is reasonable to believe that this home was targeted, and that the person or persons targeting the home sought its location and/or directions in planning this attack." Ex. 16 at 8.

Here, the totality of the circumstances—the targeting of the house, the location and characteristics of the house and the neighborhood, the planning and coordination required to carry out the crime, and the likelihood of a suspect using Google to plan and execute the crime—gave the magistrate a substantial basis for concluding probable cause existed. "[P]robable cause is a commonsense concept, objectively determined in the totality of the circumstances." *Coates*, 266 P.3d at 400 (cleaned up). "While certain facts may not establish probable cause in isolation, those same facts may support a finding of

probable cause when considered in combination." *Grassi v. People*, 2014 CO 12, ¶ 23. Probable cause existed here.

Seymour's arguments against probable cause can be distilled into two concerns: the affidavit was too speculative to establish probable cause, and there was no probable cause to search *his* account.

First, Seymour contends the affidavit is too speculative. Pet. at ¶¶ 154–58. Not so. The detective described a "specific evidential hypothesis from which a fair probability of [evidence of a crime] could be inferred." *Coates*, 266 P.3d at 400. The detective did not simply assert in a vacuum that Google might have evidence; he set forth multiple pages of factual context and experience-based observations that led to his belief that the suspects Googled the residence's address to carry out and execute the crime. "The nature of the crime, and the means by which it was committed, allow courts to make reasonable inferences about where evidence may be found." *See Arson*, 497 F. Supp. 3d at 356.

Seymour argues that the affidavit did not say the suspects were seen on the surveillance video holding or using a cell phone during

commission of the crime; thus, he contends the warrant relies on "group probabilities." The detective's evidential hypothesis was not that the suspects used a phone *during* the crime—the investigator concluded the suspects had used a device (which could be, but wasn't necessarily, a cell phone) to search Google for the address "in *planning* this attack." Ex. 16 (emphasis added).

And reliance on group probabilities is not improper. A finding of probable cause "turn[s] on the assessment of probabilities in particular factual contexts." *Gates*, 462 U.S. at 232. A probable cause determination is, by design, "based on factual and practical considerations of everyday life on which reasonable and prudent people, not legal technicians, act." *People v. Bailey*, 2018 CO 84, ¶ 21 (quoting *Mendez v. People*, 986 P.2d 275, 280 (Colo. 1999)).

The detective was entitled to draw upon his prior investigative experience in assessing probable cause in light of the factual context. "[P]olice officers . . . may use their judgment, experience, and training in evaluating the circumstances and assessing the combined importance of individual facts." *Bailey*, ¶ 20 (citation omitted). And reviewing courts

must give "[d]ue consideration . . . to a law enforcement officer's experience and training in determining the significance of the observations set forth in the affidavit." *Kerst*, 181 P.3d at 1172. Federal courts routinely "authorize[] searches and seizures of cell phones based on statements made about their use in crime grounded in the agent's training and experience." *Arson*, 497 F. Supp. 3d at 355 (collecting cases). The affidavit does not fail because the detective made inferences based on human behavior drawn from the known facts and his investigative experience.

The District Court's decision here comports with other federal courts that considered related issues involving technology. For instance, in *Arson*, 497 F. Supp.3d at 355–56, a federal district court granted a search warrant application for Google location data following a series of arsons by unknown coconspirators. The court observed that cell phones are ubiquitous and drew a reasonable inference that "suspects coordinating multiple arsons across the city in the middle of the night, as well as any passersby witnesses, would have cell phones." *Id.* The court clarified, "This is not to say that cell phones, and subsequently

location data, can be automatically searched[.]" *Id.* The affidavit "must provide sufficient information on how and why cell phones may contain evidence of the crime, as well as credible information based on the agent's training and experience, to support the assertions." *Id.*

The supporting statements in the *Arson* affidavit were similar to the detective's here. *Id.* (statements included: "it is common for criminal coconspirators to use cell phones to plan and commit criminal offenses," "there was a reasonable probability that a cell phone . . . is interfacing in some manner with a Google application, service, or platform," and "the coconspirators could have used . . . other applications to facilitate the crime, such as a GPS maps application.").

Seymour contends "[a]t the time, investigators simply 'didn't know' who they were looking for. They thought it might have been someone living in the house. They thought it might have been someone with a personal vendetta against the family. They thought it might have been a random person." Pet. at ¶ 155 (record citations omitted). This Court's review is "confined . . . to the four corners of the affidavit,"

McKay, ¶ 10, and the affidavit explained the basis for the detective's conclusions.

In any event, Seymour's argument takes the detective's testimony out of context—the detective agreed that while investigators had "thought of everything under the sun [about how] this could have happened or why this could have happened," they believed the house was targeted and the suspect likely Googled the address in planning or executing the crime. Ex. 10 at 83. Probable cause existed.

Second, Seymour contends the detective needed probable cause "with respect to the *person* to be searched." Pet. ¶ 169 (emphasis added).

Google searched its database; law enforcement did not search his "person." A third-party warrant need not identify a suspect to be valid. *See, e.g.*, *Zurcher*, 436 U.S. at 567-68 (upholding a search warrant of a newspaper office where photographs of unknown assault suspects were likely to be found). Seymour cites to *Ybarra v. Illinois*, 444 U.S. 85 (1979). In that case, law enforcement had a warrant to search a tavern and the bartender. *Ybarra*, 444 U.S. at 88–89. Officers patted down all

the patrons of the tavern, including the defendant, who had heroin in his pocket. *Id.* at 89. The Supreme Court held that law enforcement needed probable cause to search a person, which "cannot be undercut or avoided by simply pointing to the fact that coincidentally there exists probable cause to search or seize another or to search the premises where the person may happen to be." *Id.* at 91.

Seymour then relies on a geofence case that adopted the reasoning of *Ybarra*, *United States v. Chatrie*, 590 F. Supp. 3d 901 (E.D. Va. 2022).[7] In *Chatrie*, a magistrate approved a geofence warrant covering 17.5 acres for an hour during and following a bank robbery and, for any phone that left the geofence, location history for another hour beyond that. *Id.* at 919. Google executed the warrant and provided investigators with follow-up identifying information as to three users without court involvement. *Id.* at 920-21.

[7] A geofence warrant: (1) identifies a geographic area; (2) identifies a time span; and (3) requests location history data collected by Google for all users who were within that area during that time. *Id.* at 914.

The district court held the geofence warrant was invalid (although it concluded the good-faith exclusion to the exclusionary rule applied). *Id.* at 927, 936–42. Citing *Ybarra*, it found the warrant lacked probable cause because a "person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person." *Id.* at 928 (quoting *Ybarra*, 444 U.S. at 91).

But other courts addressing warrants involving novel technologies have rejected or distinguished *Ybarra*. For instance, in *Canvassing Cell-Site Simulator*, 2023 WL 1878636, at *11, the district court declined to apply *Ybarra* in analyzing probable cause for a canvassing cell-site simulator warrant.[8] It concluded that "*Ybarra* and its progeny delineate an exception to that rule for the physical bodies of persons who are present during the search of a location for which the government has obtained a warrant." *Id.* at *11. Because "capturing a signal given off by

[8] A cell-site simulator "is a device that imitates a cell tower, sending signals to nearby cellular devices, which in turn will broadcast signals that include their unique device identifiers." *Id.* at *3.

a cellular device . . . is not the same as the search of a body of a person," it found *Ybarra* inapplicable. *Id.* Instead, "[t]he correct formulation . . . is that the government must show probable cause that evidence of the crime(s) alleged will be found *in the particular place to be searched*." *Id.* (emphasis in original); *see also Arson*, 497 F. Supp. 3d at 362, n.6 (distinguishing *Ybarra* because the warrant explicitly covered the persons in the geofence whereas *Ybarra* involved a person not identified in the warrant).

Whether these courts apply *Ybarra* or not, they discuss it only because the warrant sought location data—probable cause was based on a "person's mere propinquity" to a crime. Even if *Ybarra* applies outside the context of the search of a physical body, there is no reason to apply it in this case because a reverse keyword search warrant does not identify a person by location—or, at this stage, a person at all.[9]

[9] This Court, however, has stated *Ybarra*'s principle more broadly: "[P]robable cause must exist to invade each individual's constitutionally protected interests." *Gutierrez*, 222 P.3d at 938.

The District Court applied the correct probable cause formulation here: "Probable cause exists when an affidavit for a search warrant alleges sufficient facts to warrant a person of reasonable caution to believe that contraband or evidence of criminal activity is located at the place to be searched." *Cooper*, ¶ 9. Law enforcement did not need to identify Seymour as a suspect in order to have probable cause to search Google for evidence that *someone* (whose identity would not be discovered at this stage of the warrant process) searched for the location of the house in advance of the crime. Probable cause existed here.

c. The warrant was sufficiently particular and not overbroad.

A warrant's scope is constrained by the Fourth Amendment's requirements that the warrant be sufficiently particular and not overbroad. "Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based." *Matter of Search of Info. that is Stored at Premises*

Controlled by Google LLC, 579 F. Supp. 3d 62, 75-76 (D.D.C. 2021) ("*Google D.C.*").

The search warrant clearly identified what it sought:

> For any Google accounts that conducted a search while using Google Services (i.e., Google Chrome, Google Maps, or any other Google service) using any one or more of the following the search terms:
>
> 1. "5312 Truckee"
> 2. "5312 Truckee St"
> 3. "5312 Truckee Street"
> 4. "5312 N Truckee St"
> 5. "5312 N. Truckee St."
> 6. "5312 N. Truckee St"
> 7. "5312 N Truckee St."
> 8. "5312 North Truckee"
> 9. "5312 North Truckee Street"

The warrant specified a timeframe: "For the period beginning and inclusive of July 22, 2020 at 00:01 M.S.T. through and to include August 5, 2020 at 0245 M.S.T." It instructed Google to produce "anonymized information to include the IP addresses used by all accounts that are found to have conducted any of the above[-]described keyword searches." And it constrained law enforcement to narrow down any results to those relevant to the investigation and seek further process for identifying information. Ex. 16 at 2–3.

Nonetheless, Seymour argues this detail was insufficient.

First, Seymour argues that the warrant needed to identify specific user accounts. But law enforcement was looking for evidence of specific searches made during a specific timeframe by any user. The warrant was clear, and no information was yet connected to an identified individual.

Second, Seymour contends the warrant wasn't particular enough because it didn't specify whether the results should include only exact matches of the search terms or include other words too. Pet. at ¶ 172. For instance, Google produced results "that contained additional search terms, such as state, zip code, or the word 'interior.'" Pet. at ¶ 93.

Seymour's argument is overly technical. "[H]ighly technical attacks on warrants and affidavits are not well-received," *People v. McKinstry*, 843 P.2d 18, 20 (Colo. 1993), because warrants are reviewed by a standard that values "practical accuracy rather than technical nicety." *People v. Schrader*, 898 P.2d 33, 36 (Colo. 1995). Questions about a warrant's scope inevitably arise during execution, so this Court reviews whether the description was sufficiently particular to "enable[]

the executing officer to reasonably ascertain and identify the things authorized to be seized." *Roccaforte*, 919 at 803.

Search warrants "must be tested and interpreted . . . in a commonsense and realistic fashion," but do not require "elaborate specificity." *United States v. Ventresca*, 380 U.S. 102, 108 (1965). An interpretation can still be reasonable even if it's not "the narrowest *possible* reasonable interpretation." *United States v. Aljabari*, 626 F.3d 940, 947 (7th Cir. 2010) (emphasis added).

Employing a reasonable reading of the warrant, Google could (and did) produce results for users that "conducted a search . . . using" the specified search terms.[10] A search result that included, for instance, "5312 Truckee St *Denver*" was a search conducted using the specified search term "5312 Truckee St," and the result produced was still within the scope of probable cause. The warrant did not need to be written in a legalistic fashion to survive Fourth Amendment scrutiny.

---

[10] Although review of the warrant's validity is confined to its four corners, Google explained in an affidavit what categories of data it produced. Ex. 4 ¶¶ 7, 15.

Seymour argues that the warrant's listing of Google's street address did not provide particularity. Here, the *parameters* for the search established "the place to be searched." *See Google D.C.*, 579 F. Supp. 3d at 80 (In a geofence warrant "the government has satisfied the particularity requirement as to the place to be searched because . . . it has appropriately contoured the temporal and geographic [scope]."). The parameters here told Google what to search: the specified search terms during the specified timeframe.

Finally, Seymour asserts that the warrant was overbroad because it allowed Google to search a billion accounts (plus users who were not logged in) and "did not account for the fact that someone may have conducted an address search for any number of reasons unrelated to the commission of a crime." Pet. at ¶¶ 152–65.

"[T]he proper scope of a warrant is confined to the breadth of the probable cause that supports it." *Matter of Tower Dump Data for Sex Trafficking Investigation*, No. 23 M 87, 2023 WL 1779775, at *3 (N.D. Ill. Feb. 6, 2023) ("*Sex-Trafficking*"). "Warrants that are overbroad . . . allow officers to search for items that are unlikely to yield evidence of

the crime." *United States v. Vizcarra-Millan*, 15 F.4th 473, 502 (7th Cir. 2021). "While warrants cannot be open-ended searches," they also should not be drawn so narrowly "they handcuff law enforcement's ability to execute the warrant." *Sex-Trafficking*, 2023 WL 1779775, at *6.

Seymour shifts analogies from the *Ybarra*-controlled search of a person to likening the search to looking in a billion people's apartments. Pet at ¶ 162. Conceptually, it is like neither. Google is running a query in a database, which is unlike law enforcement searching a person's body or physically rummaging through a billion people's belongings. The query provides only responsive data; no one looks at anything else. *Cf. Andresen v. Maryland*, 427 U.S. 463, 482 (1976) ("In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized."); *Coke*, ¶ 38 (suppressing a warrant that had no limitation as to what information could be seized from the defendant's cell phone).

Google's database contains vast amounts of personal data, to be sure. But this warrant called for only a narrow set of data responsive to the query for which there was probable cause, and those results contained nothing that could allow law enforcement to identify *who* conducted those searches without further warrants subject to court scrutiny.

Seymour argues that by requesting the user's IP address, it "rendered [Google's] 'de-identification' procedure meaningless and misleading" because an IP address can ultimately be connected to an individual. Pet. at ¶ 171. But further court intervention was necessary for law enforcement to obtain any person's identity. Whether the de-identification occurred through a subsequent warrant to Google, or law enforcement got a warrant for an internet service provider, a magistrate had to consider probable cause again—this time connecting a person's account to the crime with individualized probable cause—and approve another warrant before that person's identity could be revealed.

Other courts have approved of precisely this multi-step warrant process to cabin the breadth of warrants with unknown suspects. For

instance, in *Google D.C.*, the district court found "any overbreadth concerns raised by the requested geofence are further addressed by the warrant's two-step search procedure, which ensures identifying information associated with devices found within the geofence will be produced only pursuant to a further directive from the Court." *Google D.C.*, 579 F. Supp. 3d at 87; *see also United States v. Rhine*, No. CR 21-0687 (RC), 2023 WL 372044, at *32 (D.D.C. Jan. 24, 2023) (denying suppression of geofence warrant and noting "the terms of the initial warrant precluded disclosure of deanonymized device information except after separate order of the court based on a supplemental affidavit").

Seymour relies heavily on *Chatrie* in which the district court struck down a geofence warrant, but part of that court's reasoning included the fact law enforcement did not follow the process it outlined in the warrant and went directly to Google for subsequent identification of the account owners without the court's oversight. *Chatrie*, 590 F. Supp. 3d at 219. The court opined, however, that a multi-step process

with court involvement between the stages of seizing anonymized data and seizing identifying data could satisfy the Fourth Amendment:

> In certain situations, then, law enforcement likely could develop initial probable cause to acquire from Google only anonymous data from devices within a narrowly circumscribed geofence… From there, officers likely could use that narrow, anonymous information to develop probable cause particularized to specific users. Importantly, officers likely could then present that particularized information to a magistrate or magistrate judge to acquire successively broader and more invasive information.

Id. at 933. That multi-step process occurred here and appropriately cabined the breadth of the seizure.

Innocent individuals' privacy rights are often implicated in the execution of search warrants, and the Fourth Amendment's requirement that warrants not be overbroad protects those individuals' interests. "But the Fourth Amendment does not require law enforcement to use a scalpel in its investigations. The inherent nature of authorizing a search warrant is to permit law enforcement to conduct a *search for evidence* in places where there is only a *probability*, not a certainty, that evidence will be found." *Sex-Trafficking*, 2023 WL 1779775, at *4 (emphasis in original).

"The Fourth Amendment was not enacted to squelch reasonable investigative techniques because of the likelihood—or even certainty—that the privacy interests of third parties uninvolved in criminal activity would be implicated." *Google D.C.*, 579 F. Supp. 3d at 84. "[T]he fact that one uninvolved individual's privacy rights are indirectly impacted by a search is present in numerous other situations and is not unusual." *Arson*, 497 F. Supp. 3d at 361. For instance, when a house is searched pursuant to warrant, often "the entire house is subject to the search, and this includes the most private areas of a house, such as bedrooms and bathrooms, of individuals who may not be involved in the crime but who nonetheless live in the premises, such as spouses and children." *Id.* The search here was restricted so as to minimize the risk that uninvolved parties' searches were seized, and the results did not identify any person by name.

As Seymour catalogs at length, Google undeniably possesses a trove of private information about individuals that an overbroad warrant could expose. But *this* warrant does not implicate Seymour's parade of horribles. It targeted only Google searches for a residential

address, had a limited timeframe, and did not connect those searches to any individual without court approval through another warrant. These parameters are akin to those courts approved in other novel technology cases, and they follow the general principles that have applied in Fourth Amendment cases predating these technological innovations.

C. First Amendment considerations do not invalidate the warrant.

Seymour argues that Google searches implicate the First Amendment, so the District Court should have evaluated the search warrant using a more stringent test from *Tattered Cover*, 44 P.3d at 1059.

1. Legal principles

In *Tattered Cover*, law enforcement was investigating a suspected methamphetamine lab in a trailer's bedroom and discovered a mailer and invoice from the Tattered Cover bookstore in the garbage outside, addressed to one of the trailer's occupants. *Id.* at 1048. Officers executed a search warrant on the trailer and discovered two books in the bedroom relating to manufacturing drugs. *Id.* at 1049. Officers then

obtained a warrant to see if they could associate the invoice and the books in the bedroom to a suspect. *Id.* at 1050.

This Court "addressed the collision between the exercise of [the First Amendment and Article 2, Section 10 of the Colorado Constitution] and the investigative efforts of law enforcement officials." *Id.* at 1054. The First Amendment "safeguards a wide spectrum of activities, including the right to distribute and sell expressive materials, the right to associate with others, and . . . the right to receive information and ideas." *Id.* at 1051.

> Conflicts between First Amendment and Fourth Amendment rights are inevitable when law enforcement officials attempt to use search warrants to obtain expressive materials. This is because a seizure of documents, books, or films is conceptually distinct from a seizure of objects such as guns or drugs…. The former category of objects implicates First Amendment expressive rights, while the latter category of objects does not.

Id. at 1055.

The U.S. Supreme Court decided in *Zurcher*, 436 U.S. at 564, that "when expressive rights are implicated, a search warrant must comply with the particularity requirements of the Fourth Amendment with 'scrupulous exactitude.'" *Tattered Cover*, 44 P.3d at 1055. This Court

concluded, however, that "the protections afforded to fundamental expressive rights by federal law, under . . . *Zurcher* [were] inadequate." *Id.* at 1056. Thus, this Court "turn[ed] to our Colorado Constitution, [and held that it] requires a more substantial justification from the government than is required by the Fourth Amendment of the United States Constitution when law enforcement officials attempt to use a search warrant to obtain an innocent, third-party bookstore's customer purchase records." *Id.*

In this specific context, this Court adopted a balancing test:

> [T]he government, when it seeks to use a search warrant to discover customer book purchase records from an innocent, third-party bookstore, must demonstrate that it has a compelling need for the information sought. In determining whether law enforcement officials have met this standard, the court may consider various factors including whether there are reasonable alternative means of satisfying the asserted need and whether the search warrant is overly broad. The court must then balance the law enforcement officials' need for the bookstore record against the harm caused to constitutional interests by execution of the search warrant.

Id. at 1059. It noted that "in most situations, there is a lesser danger of harm to constitutionally protected interests when the customer

purchase record is sought for reasons entirely unrelated to the contents of the materials purchased by the customer." *Id.*

This Court emphasized that *Tattered Cover* "is narrow . . . and consider[ed] *only* the constitutional protections afforded when law enforcement officials seek to use a search warrant to obtain customer purchase records from a bookstore"—not "*any other type of government action that implicates expressive rights*." *Id.* at 1056, n.20 (emphasis added).

2. Analysis

a. *Tattered Cover* does not apply here.

Seymour's briefing in the District Court devoted two paragraphs to *Tattered Cover* and failed to argue how the test should be applied here, relying on his Fourth Amendment arguments. Ex. 1 at ¶ 37; Ex. 5 at ¶ 22. The District Court correctly declined to apply *Tattered Cover*.

In the twenty-one years since *Tattered Cover* was decided, no published decision in Colorado has applied—or even discussed whether to apply—that balancing test, which by its own terms applies "only" to

customer purchase records from a bookstore.[11] In dicta this Court characterized *Tattered Cover* as applying a "strict scrutiny" or "compelling need" requirement on law enforcement under the Colorado Constitution "only because the purchase records were sought specifically to discover the content or ideas contained in a particular customer's reading material." *Curious Theatre Co. v. Colorado Dep't of Pub. Health & Env't*, 220 P.3d 544, 552 (Colo. 2009); *see also Stanford v. Texas*, 379 U.S. 476, 485 (1965) (referring to federal standard, "the constitutional requirement that warrants must particularly describe the 'things to be seized' is to be accorded the most scrupulous exactitude when the 'things' are books, and the basis for their seizure is the ideas which they contain.").

Even if *Tattered Cover*'s reach was expanded beyond books, this case does not implicate the content or ideas of websites. The warrant authorized the seizure of data that one or more people searched for

---

[11] *See, e.g.*, *Coke*, ¶¶ 33–38 (holding that warrant for "all texts, videos, pictures, contact lists, [and] phone records" on suspect's cell phone was overbroad without applying *Tattered Cover*).

"5312 Truckee" (or some variation). The basis of the seizure was functional—searches for the location of the house based on its public address—rather than related to "the content or ideas contained in a particular customer's reading material." *Curious Theatre Co.*, 220 P.3d at 552.

In contrast, the basis for the seizure in *Tattered Cover* was to use the content of the drug manufacturing books to prove the perpetrator's identity and intent. *Tattered Cover*, 44 P.3d at 1047. Had investigators here sought a reverse keyword search for "how to burn down a house," to prove that a suspect burned down the house on Truckee, *Tattered Cover* would be a clearer analogue. But searching "5312 Truckee" does not raise the same concerns.

Seymour argues that searching for certain commercial street addresses, like Planned Parenthood's, "can be revealing." Pet. at ¶ 111. But a person isn't engaging in the "marketplace of ideas" by looking up an address on a map, as compared to, say, engaging in speech or research about Planned Parenthood's services. The traditional Fourth Amendment analysis adequately protects an individual from the

government learning who Googled particular addresses because there must be probable cause, particularity, and the nexus between the criminal activity and the scope of the warrant. In addition, probable cause particularized to the person must be found before a particular Google search can be connected to an identifiable person.

b. Alternatively, *Tattered Cover*'s balancing test was satisfied.

Seymour did not develop a cogent argument applying the *Tattered Cover* factors either in the District Court briefing or here. Ex. 1 at ¶ 37; Ex. 5 at ¶ 22; Pet. at ¶ 104. He failed to discuss law enforcement need, reasonable alternative means for gaining the information, or how to balance those against any chilling effect. This Court should decline to address arguments raised in only a cursory, conclusory, or perfunctory fashion. *See People v. Mershon*, 874 P.2d 1025, 1035 n. 13 (Colo. 1994).

If the District Court should have applied *Tattered Cover*'s balancing test, however, the record supports upholding the warrant because (1) there was a compelling need for the information sought and no other reasonable alternative means of satisfying the need for the

information; (2) the warrant was not overbroad; and (3) the potential harm caused to constitutional interests by execution of the search warrant was limited under the circumstances.

First, law enforcement had a compelling need for the information sought and lacked other reasonable alternative means. The crime was extremely serious—a fire that appeared to be intentionally set killed five people and injured three others. The investigation revealed three coconspirators captured on video in the yard moments before the fire broke out, and arson investigators found evidence of an accelerant used inside the house.

Before seeking this search warrant, investigators exhausted other investigative techniques. They interviewed the surviving victims, canvassed the neighborhood, and reviewed neighbors' surveillance footage. Ex. 3 at 2; Ex. 9 at 42–43. Most physical evidence was destroyed in the fire, and five of the house's nine occupants were dead. Ex. 9 at 34, 109.

Investigators also explored other technological methods of investigating, including trying to determine whether a suspects' phone

connected to any nearby homes' wifi routers, obtaining warrants for "tower dumps" that identified all cell phones in the area at the time of the crime, and obtaining a warrant for a cell site simulator that determined what cell phones were in the area to compare and exclude devices from the tower dumps. Ex. 1 at ¶ 87; Ex. 9 at 46–47, 121–30.

Investigators had reached an impasse; three unknown suspects remained at large in the community. Accordingly, law enforcement had significant need for this information, and no other reasonable means for identifying the suspects.

The need for the customer information in *Tattered Cover* was far less significant. This Court observed that the defendant's intent could alternatively be demonstrated by evidence of "a fully operational and functional methamphetamine lab as well as a small quantity of the manufactured drug" with two "how-to" books in the vicinity, and perpetrator's identity could be proven by looking at the bedroom's clothing, furniture, papers, or personal objects; checking objects for fingerprints; or searching the bedroom for DNA samples. *Tattered Cover*, 44 P.3d at 1061. None of those possibilities existed here.

Second, the warrant was not overbroad. As previously discussed, the warrant sought extremely limited information—data associated with as-yet unidentified users who searched for the house's address in the fifteen days before the crime.

Finally, the chilling effect was limited under the circumstances here. Law enforcement's interest in the address was unrelated to the content of any website a user might have accessed after searching "5312 Truckee." It sought the record to determine who might have Googled the address while formulating a plan to burn the house down. This is the type of search that this Court identified in *Tattered Cover* as having a "minimal" harm on the public. *Id.* at 1059. "If the government seeks a purchase record to prove a fact unrelated to the content or ideas of the book," such as placing a suspect at a scene or disproving an alibi, "then the public's right to read and access these protected materials is chilled less than if the government seeks to discover the contents of the books a customer has purchased." *Id.* People should be free to "discover and consider the full range of expression and ideas available in our 'marketplace of ideas,'" but looking for directions to a residential

address on the internet is not the kind of activity that is likely to be chilled. *Id.* at 1052.

The motion to suppress was properly denied.

IV. Law enforcement relied on the search warrant in good faith.

A. Standard of review and preservation.

The People invoked the good-faith exception to the exclusionary rule before the District Court. Ex. 3 at 9. Although the District Court upheld the reverse keyword search warrant, it also made factual findings relevant to the good-faith exception. Ex. 8 at 28–29. Those factual findings are afforded deference, and should not be overturned "if they are supported by competent evidence in the record." *Cooper*, ¶ 7.

B. Even if the warrant is invalidated, the motion to suppress should be denied.

1. Legal principles

When a reviewing court later finds that a magistrate judge lacked a substantial basis for issuing a search warrant, exclusion does not necessarily follow. "The exclusionary rule is a judicially created remedy designed to safeguard Fourth Amendment rights generally through its

deterrent effect." *Cooper*, ¶ 7; *see also McKnight*, ¶ 61 (holding the exclusionary rule applies to evidence obtained in violation of the Colorado Constitution). "Because the exclusionary rule is intended to deter improper police conduct, it should not be applied in cases where the deterrence purpose is not served[.]" *Casillas v. People*, 2018 CO 78M, ¶ 21.

One such case is where a search occurred pursuant to a valid warrant, approved by a magistrate. This "good-faith exception" to the exclusionary rule allows a trial court to admit evidence that was obtained in good faith reliance on a warrant, even if the warrant is later deemed invalid. *Cooper*, ¶ 10; *Gutierrez*, 222 P.3d at 941 ("The exclusionary rule is aimed at deterring the misconduct of police officers, not magistrates.").

In Colorado, the exception is codified at § 16-3-308(4), C.R.S. (2022). Under that section, evidence that would otherwise be subject to the exclusionary rule will not be suppressed if it was obtained by an officer who had "a reasonable, good faith belief that [their conduct] was proper." § 16-3-308(4)(a). In making this determination, the search

occurring "pursuant to and within the scope of a warrant" is prima facie evidence of the executing officer's reasonable good faith "unless the warrant was obtained through intentional and material misrepresentation." § 16-3-308(4)(b).

The presumption created by § 16-3-308(4)(b) "may be rebutted if the officer failed to undertake the search in an objectively good faith belief that it was reasonable." *Cooper*, ¶ 11 (quoting *People v. Miller*, 75 P.3d 1108, 1112 (Colo. 2003)). To do so, a defendant must show (1) that the "issuing magistrate was misled by a known or recklessly made falsehood," (2) that the warrant was "so facially deficient that the officer cannot reasonably determine the particular place to be searched or things to be seized," or (3) that the warrant was "based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Miller*, 75 P.3d at 1114 (citing *United States v. Leon*, 468 U.S. 897, 906 (1984)).[12]

---

[12] *Miller* also indicated that the presumption of good faith could be rebutted where "the issuing magistrate wholly abandoned the judicial role." 75 P.3d at 1114. The Petition disclaims reliance on this option. Pet. ¶ 179.

2. Should the Court conclude the magistrate erred in approving the reverse keyword warrant, this case presents a textbook application of the good-faith exception.

Early in its oral ruling on Seymour's Motion to Suppress, the District Court paused to discuss the purpose of the exclusionary rule, and the "corollary" of how courts should react "when the police actually do exactly what we ask them to do, i.e., resort to the judicial process to get authorization." Ex. 8 at 16. The District Court found that, in this case "the police [did] exactly what we want the police to do." *Id.* at 17. When their investigation led them to searches "that implicate Fourth Amendment issues," they went "first to the courts to obtain authorization to do so." *Id.*

The District Court returned to this sentiment throughout its ruling. *See, e.g.*, *id.* at 22–23, 28–29 (finding "in passing" that if it had had chosen to invalidate the warrant it "would defy common sense and comprehension to believe . . . that somehow any of the criteria for the good-faith exception would come into play that would not allow that

exception to be applicable"). Ultimately, it concluded, "based on [its] review" of the case:

> [I]t is my judgment that the police in this case did exactly what we want the police to do, i.e., be careful, be specific, be particular in terms of judicial process to obtain this information . . . I think the police here did exactly what we want them to do.

Id. at 43.

This case presents a textbook application of the good-faith exception. Despite advancing third-party doctrine arguments before the District Court, *see infra* Part II, law enforcement did not rely on that interpretation of the U.S. and Colorado Constitutions. They went to a magistrate and obtained a warrant. And when Google raised anonymization concerns with the initial—and second—warrants, law enforcement worked diligently to address those concerns. Each time requesting, and obtaining, a judicially-approved warrant.

Ultimately, law enforcement layered multiple rounds of judicial review into the investigatory process. The police obtained one warrant to conduct the initial reverse keyword search. Ex. 16. After reviewing the anonymized records returned under that warrant, the police sought

and obtained a second warrant requesting further information about specific users. Ex. 18. At each stage, law enforcement worked within the confines of the legal process, not outside it.

None of the grounds not to apply the good-faith exception are applicable here.

First, law enforcement did not mislead the magistrate. The Petition suggests that law enforcement knowingly or recklessly "omitted critical information about the unprecedented scope" of this warrant, namely that it would "entail the search of billions of people." Pet. at 91–92. But the District Court concluded that "that's just not what the search warrant does, and there would be no obligation to put that in a search warrant or affidavit because it's not true." Ex. 8 at 27. *See also United States v. Tutis*, 216 F. Supp. 3d 467, 482 (D.N.J. 2016) (finding an affidavit for a cell-site simulator was not misleading even though it did not use the words "cell-site simulator" but described what the technology did and did not do).

Nor does the warrant's invocation of the Stored Communications Act (SCA) invalidate its probable cause. Pet. at 96–98. Regardless of

whether the warrant was adequate under the SCA, it was issued and upheld under Colorado law. § 16-3-301, C.R.S. (2022); Ex. 16 at 2657. An SCA analysis is unnecessary.

Next, the warrant did call for "deidentified" results, and the warrant's assertion of such was not "empty and misleading." Pet. at 98. It is undisputed that law enforcement needed, and obtained, an additional warrant to identify the users who ran these searches. *See* Ex. 10 at 86–88. Just because law enforcement could ultimately turn an IP address into an identity—with further judicial authorization—does not render the original return from Google "deidentified."

Finally, as discussed above, that Google refused to comply with two previous warrants is immaterial to the calculus of whether the third warrant establishes probable cause. Pet. at 99. Google's policies are not constitutional mandates, and regardless, the question before Judge Zobel was whether the third warrant established probable cause. Google's refusal to comply with previous warrants based on its own commercial policies is irrelevant to that question.

Second,[13] as explained in above, the warrant contained was not so facially deficient that "official belief [that probable cause existed] is unreasonable." *Gutierrez*, 222 P.3d at 941. Nor was the warrant so "bare bones" as to undermine the good-faith exception. *Id.*

Most often, a bare-bones affidavit is one that relies on conclusory statements. *Gutierrez*, 222 P.3d at 941. "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 also too "bare bones" to invoke the good-faith exception. *Id.*

Neither describes the affidavit here. The District Court called it "one of the more detailed and specific and narrowly tailored affidavits that this Court really has encountered in a long time." Ex. 8 at 26. Over the course of several pages, it exhaustively detailed the investigation leading up to the warrant, and how the reverse keyword search warrant fit into that investigation. Ex. 16.

---

[13] Although the Petition separates the third and fourth reasons why the good-faith exception may not apply in a given case, and transposes them from how they appear in the caselaw, *compare Cooper*, ¶ 12 *with* Pet. at 101, 104, the District Court addresses them here together.

But the affidavit did not just describe the state of the investigation. It also provided a nexus between what that investigation had uncovered and the place to be searched. *See Gutierrez*, 222 P.3d at 942. The affiant explained why, based on his training and experience, he believed the home had been specially targeted. Ex. 16 at 8. He then explained why, based on that same training and experience, he concluded that the perpetrators likely searched for the home and "sought its location and/or directions" to it. *Id.*

Finally, and perhaps most importantly for good faith purposes, three separate judicial officers have now concluded that the affidavit established probable cause. *See Gutierrez*, 222 P.3d at 942 (holding that courts may consider, in addressing the good-faith exception, whether judges "are divided on the question of probable cause"). Prior to the warrant at issue here, a different magistrate judge, Judge Faragher, approved two earlier versions of the keyword search warrant based on

virtually identical affidavits.[14] Exs. 12, 14. And, of course, the District Court also found that this affidavit was sufficient to establish probable cause. Ex. 8 at 26.

Notably, this search warrant addressed a novel legal issue. No case, federal or state, has determined the validity of a reverse keyword search warrant. The purpose of the exclusionary rule is not served by excluding evidence when law enforcement sought court approval before using a novel investigative technique.

Chatrie, on which the Petition relies, is instructive. After invalidating the warrant there, the Court nonetheless declined the motion to suppress. It concluded that prior to its ruling, "the legality of this investigative technique was unclear," and "the permissibility of geofence warrants is a complex topic, requiring a detailed, nuanced understanding and application of Fourth Amendment principles, which

---

[14] These two previous incarnations are in addition to Judge Zobel's approval of the warrant that was actually executed. *But see Gutierrez*, 222 P.3d at 942 ("[C]ourts may not consider the magistrate judge's initial decision to issue the warrant" in assessing whether law enforcement's reasonable reliance on the magistrate's probable cause determination).

police officers are not and cannot be expected to possess." *Chatrie*, 590 F. Supp. 3d at 938.[15] Like numerous other courts, the *Chatrie* court recognized that the novelty of the investigative technique in question weighed in favor of applying the good-faith exception. *See, e.g. United States v. Levin*, 874 F.3d 316, 323 (1st Cir. 2017) ("We see no benefit in deterring [the police from seeking search warrants where new technology is implicated]—if anything, such conduct should be encouraged, because it leaves it to the courts to resolve novel legal issues."); *United States v. Daprato*, No. 2:21-CR-00015-JDL-4, 2022 WL 1303110, at *8 (D. Me. May 2, 2022) (applying the good-faith exception because "[c]ourts should not punish law enforcement officers who are on the frontiers of new technology"); *United States v. Wellman*, No. CRIM A 1:08CR00043, 2009 WL 37184, at *7 (S.D.W. Va. Jan. 7, 2009) ("[L]aw enforcement officers utilizing relatively new technology and innovative

---

[15] Here, law enforcement also consulted with a district attorney—who signed the warrant application too. Ex. 16 at 9. *See also Chatrie*, 590 F. Supp. 3d at 938 ("While magistrate approval and consultation with the prosecution alone cannot and should not mechanically trigger the good-faith exception, exclusion here likely would not 'meaningfully deter' improper law enforcement conduct.")

techniques in good faith should not be penalized with suppression of important evidence simply because they are at the beginning of a learning curve and have not yet been apprised of the preferences of courts on novel questions.").

Taken together, law enforcement here was justified in relying on Judge Zobel's conclusion that the reverse keyword warrant established probable cause. Law enforcement availed themselves of the judicial process at every stage of this investigation. And even if the Court invalidates the warrant, that justified reliance precludes suppression.

CONCLUSION

The rule to show cause should be discharged.

Respectfully submitted on this 7th day of March, 2023.

NATALIE HANLON LEH
Chief Deputy Attorney General

/s/ *Trina K. Kissel*
/s/ *Peter G. Baumann*

TRINA K. KISSEL, 47194*
Senior Assistant Attorney General
PETER G. BAUMANN, 51620*
Assistant Attorney General
Attorneys for Respondent
**Counsel of Record for Denver District Court*

CERTIFICATE OF SERVICE

This is to certify that I have duly served the within **THE DISTRICT COURT'S RESPONSE TO THE ORDER TO SHOW CAUSE** upon all parties herein by Colorado Courts E-filing (CCE) or by depositing copies of same in the United States mail, first-class postage prepaid, at Denver, Colorado, this 7th day of March 2023.

/s/ *Trina K. Kissel*