DATE FILED: October 16, 2023
CASE NUMBER: 2023SA12

ADVANCE SHEET HEADNOTE
October 16, 2023

2023 CO 53

No. 23SA12, *People v. Seymour*—Fourth Amendment—Searches and Seizures—Internet—Probable Cause—Expectation of Privacy—Possessory Interests—Particularity—Nexus—Warrants—Good Faith—First Amendment—Expressive Conduct.

Exercising its original jurisdiction under C.A.R. 21, the supreme court addresses the constitutionality of law enforcement's use of a reverse-keyword warrant to obtain from Google certain user-account data related to a suspected arson that resulted in the deaths of five people. The court discharges its rule to show cause for several reasons. First, the court concludes that, under the Colorado Constitution, the defendant has a constitutionally protected privacy interest in his Google search history even when revealed only in connection with his IP address and not his name and that, under both the Colorado Constitution and the Fourth Amendment, he also has a constitutionally protected possessory interest in that same history. Second, the court concludes that the defendant's Google search history implicates his right to freedom of expression; thus, the constitutional protections must be applied with "scrupulous exactitude." *Zurcher v. Stanford*

Daily, 436 U.S. 547, 564 (1978) (quoting *Stanford v. Texas*, 379 U.S. 476, 485 (1965)). Third, a majority of the court concludes that the warrant at issue adequately particularized the place to be searched and the things to be seized. Fourth, the majority assumes without deciding that the warrant required individualized probable cause and that its absence here rendered the warrant constitutionally defective. Finally, the majority concludes that law enforcement obtained and executed the warrant in good faith, so the evidence shouldn't be suppressed under the exclusionary rule.

The Supreme Court of the State of Colorado
2 East 14th Avenue • Denver, Colorado 80203

2023 CO 53

Supreme Court Case No. 23SA12
Original Proceeding Pursuant to C.A.R. 21
District Court, City and County of Denver, Case No. 21CR20001
Honorable Martin F. Egelhoff, Judge

In Re
Plaintiff:

The People of the State of Colorado,

v.

Defendant:

Gavin Seymour.

Rule Discharged
en banc
October 16, 2023

Attorneys for Plaintiff:
Beth McCann, Denver District Attorney
Katherine A. Hansen, Senior Deputy District Attorney
Joseph M. Morales, Chief Deputy District Attorney
Courtney L. Johnston, Chief Deputy District Attorney
Denver, Colorado

Attorneys for Defendant:
Stinson Law Office
Jenifer Stinson
Denver, Colorado

The Juba Law Office, PLLC
Michael S. Juba
Denver, Colorado

National Association of Criminal Defense Lawyers
Michael W. Price
Washington, District of Columbia

Attorneys for Respondent District Court, City and County of Denver:
Natalie Hanlon Leh, Chief Deputy Attorney General
Trina K. Kissel, Senior Assistant Attorney General
Peter G. Baumann, Assistant Attorney General
Denver, Colorado

Attorneys for Amicus Curiae Colorado Attorney General:
Philip J. Weiser, Attorney General
Jillian J. Price, Deputy Attorney General
Helen Norton, Special Assistant Attorney General
Brock J. Swanson, Senior Assistant Attorney General
Matthew J. Worthington, Assistant Attorney General
Denver, Colorado

Attorneys for Amicus Curiae Colorado District Attorneys' Council:
Kevin E. McReynolds, Senior Appellate Deputy District Attorney
Golden, Colorado

Thomas R. Raynes
Denver, Colorado

Attorneys for Amicus Curiae Electronic Frontier Foundation:
Proff Law, LLC
Hannah Seigel Proff
Denver, Colorado

Jennifer Lynch
San Francisco, California

Attorneys for Amicus Curiae Electronic Privacy Information Center:
Calli Schroeder
Washington, District of Columbia

JUSTICE HOOD delivered the Opinion of the Court, in which **CHIEF JUSTICE BOATRIGHT**, **JUSTICE GABRIEL**, and **JUSTICE HART** joined.
JUSTICE BERKENKOTTER concurred in the judgment.
JUSTICE MÁRQUEZ, joined by **JUSTICE SAMOUR**, dissented.

JUSTICE HOOD delivered the Opinion of the Court.

¶1 Two months after an apparent arson left five people dead, the Denver Police Department ("DPD") still had no suspects. Their leads exhausted, they employed an unconventional investigative technique: a "reverse-keyword warrant." After some back and forth about the language in the warrant, Google disclosed to DPD a list that included five Colorado internet protocol ("IP") addresses associated with devices that had searched for the location of the fire in a roughly two-week period before it occurred. Based in part on this information, law enforcement eventually charged Gavin Seymour and two others with multiple counts of first degree murder.

¶2 Before trial, Seymour moved to suppress the fruit of the warrant, arguing that it lacked two essential constitutional ingredients: probable cause and particularity. The trial court denied Seymour's suppression motion. We granted Seymour's petition to review that order by issuing a rule to show cause.

¶3 We discharge the rule to show cause (and thus, essentially affirm the trial court's order), albeit on slightly different grounds. First, we conclude that, under the Colorado Constitution, Seymour has a constitutionally protected privacy interest in his Google search history even when revealed only in connection with his IP address and not his name and that, under both the Colorado Constitution and the Fourth Amendment, he also has a constitutionally protected possessory

interest in that same history. Second, we conclude that Seymour's Google search history implicates his right to freedom of expression; thus, the constitutional protections must be applied with "scrupulous exactitude." *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (quoting *Stanford v. Texas*, 379 U.S. 476, 485 (1965)). Third, we conclude that the warrant at issue adequately particularized the place to be searched and the things to be seized. Fourth, we assume without deciding that the warrant required individualized probable cause and that its absence here rendered the warrant constitutionally defective. Finally, we conclude that law enforcement obtained and executed the warrant in good faith, so the evidence shouldn't be suppressed under the exclusionary rule.

¶4 In reaching these conclusions, we make no broad proclamation about the propriety of reverse-keyword warrants. As is often true when we examine what is reasonable under the search-and-seizure provisions of the federal and state constitutions, much is fact-dependent. Our finding of good faith today neither condones nor condemns all such warrants in the future. If dystopian problems emerge, as some fear, the courts stand ready to hear argument regarding how we should rein in law enforcement's use of rapidly advancing technology. Today, we proceed incrementally based on the facts before us.

I. Facts and Procedural History

¶5 On August 5, 2020, a fire broke out at a Denver home, killing five people. Investigators suspected arson because they concluded that an accelerant had been used to start the fire, and a neighbor's home-security surveillance footage showed three masked individuals with what appeared to be a gas canister at the house when the fire started.

¶6 In the following weeks, DPD investigators interviewed neighbors, reviewed surveillance footage from nearby gas stations, and obtained at least twenty-three search warrants, but these efforts proved unfruitful. After more than two months of rigorous investigation, law enforcement had exhausted all their leads without identifying a single suspect.

¶7 Despite this dead end, investigators surmised that the perpetrators had intentionally targeted the address. In pursuing this theory, they inferred that the perpetrators would have researched the property before burning it down or, at the very least, looked up directions to get there. So, investigators sought and obtained a series of reverse-keyword warrants, which required Google, the dominant search-engine company, to identify users who had searched the address within a specified period.[1]

[1] Reverse-keyword warrants operate differently than traditional warrants. With traditional warrants, investigators first identify a suspect or suspects, then obtain

¶8 The first warrant requested a list of any users who had searched one of nine variations of "5312 N. Truckee St.," the address in question, in the fifteen days before the fire. Investigators sought each user's full name, date of birth, email address, physical address, phone number, and IP address.[2]

¶9 Google's privacy policies, however, stood in the way. In a sworn declaration to the trial court, a Google policy specialist explained that, to protect its users' legal and privacy interests, Google uses a staged process to respond to warrants. The company first provides law enforcement with a "de-identified," or anonymized, list of responsive searches. Then, if law enforcement concludes that any of the anonymous results are relevant to the investigation, Google will identify the users if court-ordered to do so. Because the first warrant here ordered Google to immediately produce identifying information, complying with the warrant

---

a warrant to search them or their property for evidence. However, reverse-keyword warrants start with a potentially incriminating piece of evidence—a search term like the address where the alleged arson occurred—then request a list of users implicated by that evidence. *See* Corin Faife, *Powerful Keyword Warrants Face New Challenge in Deadly Arson Case*, The Verge (July 1, 2022), https://www.theverge.com/2022/7/1/23191406/denver-arson-google-keyword-warrant-challenge-constitutional-fourth-amendment-privacy [https://perma.cc/PT8W-7CWV].

[2] "An IP address is a unique string of (often randomized) numbers assigned to an individual computer or local network" that can "help identify a specific user or a user's location while on the internet." *IP Address Explained: What Is an IP Address?*, Intuit Mailchimp, https://mailchimp.com/resources/ip-address-explained (last visited October 12, 2023) [https://perma.cc/Z4NH-MFHT].

would have violated Google's policies. So, the company refused to produce the requested records. Ultimately, DPD withdrew the first warrant.

¶10 DPD then obtained a second warrant seeking the same list of users. Instead of requesting personally identifying information like names and birth dates, DPD requested two days of location data for each account. Google again refused to comply because of privacy concerns, and investigators again withdrew the warrant.

¶11 Finally, to address Google's concerns, law enforcement obtained a third warrant, requesting that Google produce an anonymized list containing "an identifier assigned by Google representing each device . . . along with the associated IP address" "[f]or any Google accounts that [searched the address during the fifteen-day period before the fire] while using Google Services (i.e., Google Chrome, Google Maps, or any other Google service)." Google complied with this third warrant and produced a spreadsheet of sixty-one searches made by eight accounts.

¶12 Five of the eight accounts had Colorado-based IP addresses. DPD then successfully retrieved the names and other personal information associated with those five Colorado accounts through another warrant, to which Google submitted without objection. One individual was eliminated as a suspect because she was related to the alleged victims. DPD also sent warrants to social media platforms

and internet service providers to obtain information about the remaining four people. Based on this information, DPD was able to rule out another suspect.

¶13 Seymour, one of the remaining three suspects, was eventually charged with numerous felonies, including multiple counts of first degree murder, arson, and burglary.

¶14 Before trial, Seymour moved to suppress all evidence resulting from the search executed under the reverse-keyword warrant, arguing that it was unconstitutional because it was not adequately particularized and lacked individualized probable cause. The trial court denied Seymour's motion.

¶15 Seymour then filed a C.A.R. 21 petition asking us to intervene, and we issued a rule to show cause.[3]

II. Analysis

A. Original Jurisdiction under C.A.R. 21

¶16 The decision to exercise original jurisdiction under C.A.R. 21 "is an extraordinary remedy limited in purpose and availability," *People v. Owens*, 2018 CO 55, ¶ 4, 420 P.3d 257, 258, and rests within this court's sole discretion, *People v. Kelley*, 2023 CO 32, ¶ 22, 530 P.3d 407, 412. We exercise original

[3] We agreed to review the following issue:

> Whether a "reverse keyword warrant" violates the Fourth Amendment of the United States Constitution and Article II, Section 7 of the Colorado Constitution.

jurisdiction when "an appellate remedy would be inadequate, a party may suffer irreparable harm, or a petition raises an issue of first impression that has significant public importance." *People v. A.S.M.*, 2022 CO 47, ¶ 9, 517 P.3d 675, 677.

¶17 The constitutionality of reverse-keyword warrants presents an issue of first impression in Colorado. Indeed, to our knowledge, no state supreme court or federal appellate court has addressed the constitutionality of such warrants.[4] Nor have we previously determined whether individuals have a reasonable expectation of privacy in their internet search history.

¶18 Given this novelty, the ubiquity of the technology at issue, the potential for the issue to recur, and the privacy interests at stake, we choose to intervene now.

B. Standard of Review

¶19 Whether evidence should be suppressed is a mixed question of law and fact. *People v. Thompson*, 2021 CO 15, ¶ 15, 500 P.3d 1075, 1078. As a result, we defer to the trial court's factual findings if they are supported by competent evidence, but we review the legal effect of those findings de novo. *Id.*

---

[4] While the legal issue is novel, law enforcement's use of this investigative tool is not. Of course, Google's protocol here implies as much. But secondary legal authority reveals more. Google has worked with law enforcement to produce nominally anonymized lists in many other cases as well. *See* Helen Winters, Note, *An (Un)reasonable Expectation of Privacy? Analysis of the Fourth Amendment When Applied to Keyword Search Warrants*, 107 Minn. L. Rev. 1369, 1387–89 (2023) (describing Google's standard process for addressing reverse-keyword warrants, sometimes including slight variations of what we see here).

C. Constitutionally Protected Search-and-Seizure Interests

¶20 The United States and Colorado Constitutions protect individuals against "unreasonable searches and seizures." U.S. Const. amend. IV; Colo. Const. art. II, § 7. A "search" occurs when the government infringes on an individual's reasonable expectation of privacy, *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring), and "[a] 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property," *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). *See also People v. McKnight*, 2019 CO 36, ¶ 30, 446 P.3d 397, 404 (recognizing Colorado's long-standing application of this Fourth Amendment framework under article II, section 7 of the Colorado Constitution). So, for Seymour to have standing to assert a claim in this context, he must have a reasonable expectation of privacy in the place to be searched or a possessory interest in the property seized. *Rakas v. Illinois*, 439 U.S. 128, 139–40 (1978) (explaining that traditional standing inquiries, such as whether the proponent of a legal right has alleged an "injury in fact" and is asserting his own legal rights and interests, are subsumed by substantive law under the Fourth Amendment; the relevant inquiry is whether the disputed search has infringed on an interest that the Amendment protects); *see also People v. Oates*, 698 P.2d 811, 815 (Colo. 1985) (applying the same standing principles under the

Colorado Constitution). With these concepts in mind, we turn to the facts of this case.

1. The Search: A Reasonable Expectation of Privacy

¶21 At the suppression hearing, the trial court concluded that Seymour had a reasonable expectation of privacy in his Google search history. But the trial court didn't identify whether this conclusion was rooted in the federal or the state constitution. And as we explain below, this distinction matters because the Fourth Amendment and article II, section 7 of the Colorado Constitution recognize different scopes of privacy interests.[5] However, under both constitutions, the initial framework for analyzing an alleged privacy interest is the same, so we turn to that framework now.

¶22 Courts use a two-prong test to determine if a claimed privacy interest warrants constitutional protection: (1) whether the individual "exhibited an actual

[5] The prosecution, in its briefing to this court, asserts that the fact that DPD obtained a search warrant makes it unnecessary to decide the "murky" question of whether Seymour had a reasonable expectation of privacy in the searches he conducted on a third-party application or website. *See United States v. Rhine*, No. CR 21-0687 (RC), 2023 WL 372044, at *27 (D.D.C. Jan. 24, 2023) (addressing geofence warrants, which cast a virtual net around a specific location during a narrow timeframe, and declining to reach the issue of Fourth Amendment standing because it resolved the suppression motion on other grounds). But in the interest of making this threshold issue less murky, we address it now. Moreover, if Seymour has no standing to assert a claim under either the federal or state constitution, then the validity of the warrant would become moot and most of this opinion would be academic.

(subjective) expectation of privacy" and (2) whether, objectively, "the expectation [is] one that society is prepared to recognize as 'reasonable.'" *People v. Gutierrez*, 222 P.3d 925, 932 (Colo. 2009) (alteration in original) (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring)); *see Oates*, 698 P.2d at 814 (applying the same test under the Colorado Constitution).

¶23 The first (or subjective) prong is an "important, but not dispositive, element." *Gutierrez*, 222 P.3d at 932. Here, Seymour evinced his subjective expectation of privacy in his Google search history by using a search engine with strict privacy protections. Google stores user data in an encrypted database, and nothing in the record indicates that Seymour took action to make his data public. Moreover, Google takes stringent measures to ensure unauthorized individuals, including its own employees and contractors, do not access user data. As in *Gutierrez*, which we discuss at greater length below, Seymour was "entitled to assume that" his search history would "not be broadcast to the world." *Id.* (quoting *Katz*, 389 U.S. at 352); *see also Bowers v. Cnty. of Taylor*, 598 F. Supp. 3d 719, 730 (W.D. Wis. 2022) (recognizing the defendant's subjective expectation of privacy where he had taken "some steps" to keep his account private).

¶24 The second (or objective) prong more typically dictates whether constitutional protections apply. *Gutierrez*, 222 P.3d at 932. In considering what constitutes a reasonable expectation in this digital context, courts must consider

not only the precise technology at issue, but also "more sophisticated systems that are already in use or in development." *Carpenter v. United States*, 138 S. Ct. 2206, 2218–19 (2018) (quoting *Kyllo v. United States*, 533 U.S. 27, 36 (2001)). The government cannot leave citizens "at the mercy of advancing technology" by skirting warrant requirements with new tools. *Id.* at 2214 (quoting *Kyllo*, 533 U.S. at 35).

¶25 In *Carpenter*, for example, the Supreme Court held that individuals have a reasonable expectation of privacy in their cell site location information ("CSLI"), data collected by a phone company tracking its users' movements. *Id.* at 2217. The Court reasoned that an individual's 127-day location history provided an "intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" *Id.* (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

¶26 Like the location data in *Carpenter*, an individual's Google search history "hold[s] for many Americans the 'privacies of life.'" *Id.* (quoting *Riley v. California*, 573 U.S. 373, 403 (2014)). For example, CSLI may indicate that an individual regularly attends a religious service or a therapy group, has children at a particular school, or is undergoing certain medical treatments. Similarly, online search history may indicate an individual's interest in a specific religion or research into

sensitive medical conditions, information that could reveal intimate details about an individual's private life. The contents of an individual's internet searches reveal as much, if not in many instances more, about one's private life than other records in which we've previously held individuals have a reasonable expectation of privacy. *See People v. Sporleder*, 666 P.2d 135, 143–44 (Colo. 1983) (holding that, in contrast to the federal constitution, the Colorado Constitution ensures a reasonable expectation of privacy in telephone records); *Charnes v. DiGiacomo*, 612 P.2d 1117, 1121 (Colo. 1980) (same for financial records); *cf. United States v. Soybel*, 13 F.4th 584, 591–94 (7th Cir. 2021) (distinguishing CSLI from pen register data because the latter reveals nothing about the contents of the communications and doesn't, therefore, reveal the privacies of life in the same way as CSLI).

¶27 Digital privacy laws further demonstrate that society finds an expectation of privacy in digital data to be objectively reasonable. In 1986, Congress passed the Stored Communications Act ("SCA"), which provided a layer of protection for digital data in the years before *Carpenter* was decided. *See* 18 U.S.C. §§ 2701–2713 (2018); Matthew Tokson, *The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018–2021*, 135 Harv. L. Rev. 1790, 1841–42 (2022) (arguing that *Carpenter* now provides even greater protection than the SCA). And in 2021, the state legislature passed a comprehensive privacy law creating personal data privacy rights. *See* Colorado Privacy Act, §§ 6-1-1301 to -1313, C.R.S. (2023).

¶28 But we must be mindful that Google's multi-step process here first yielded only nominally anonymized IP addresses, which identified computerized devices, or potentially networks, from which users initiated the relevant searches. Google provided law enforcement no names or other personally identifying information until investigators subsequently obtained another warrant asking Google to link the IP addresses to the names of the Colorado users. So, even if we determine that individuals have a privacy interest in their internet search histories, we must further consider whether that privacy interest encompasses those histories when viewed simply in connection with an anonymized IP address.

¶29 Many federal courts say no. Under the federal constitution, courts have generally held that individuals have no reasonable expectation of privacy in data that is revealed to, and then collected and stored by, a third party. *See United States v. Miller*, 425 U.S. 435, 443 (1976) (holding that individuals have no reasonable expectation of privacy in their bank records); *Smith v. Maryland*, 442 U.S. 735, 745–46 (1979) (same for telephone numbers dialed from an individual's phone); *cf. Carpenter*, 138 S. Ct. at 2216 (recognizing individuals' privacy interests in CSLI even though that data is collected and stored by a third-party phone company). Despite *Carpenter* casting some doubt on the doctrine's overall reach, this so-called "third-party doctrine" still constrains individuals' reasonable expectations of privacy in digital data shared with third parties. *See,*

e.g., *Bowers*, 598 F. Supp. 3d at 729–32 (applying the third-party doctrine despite "[t]he uncertainty in the law" regarding individuals' privacy interests in digital data post-*Carpenter*). Thus, most federal courts continue to reject the notion that an individual such as Seymour has a reasonable expectation of privacy in information shared with a third-party vendor, whether shared by name or IP address. *See, e.g.*, *United States v. Rosenow*, 50 F.4th 715, 737–38 (9th Cir. 2022); *Soybel*, 13 F.4th at 591–94; *United States v. Hood*, 920 F.3d 87, 92 (1st Cir. 2019); *Heeger v. Facebook, Inc.*, 509 F. Supp. 3d 1182, 1189–90 (N.D. Cal. 2020).

¶30 But this is where Colorado parts ways with the Fourth Amendment. *See McKnight*, ¶ 38, 446 P.3d at 406 (recognizing that, "despite the substantial similarity between article II, section 7 and the Fourth Amendment, 'we are not bound by the United States Supreme Court's interpretation of the Fourth Amendment when determining the scope of state constitutional protections'" (quoting *Sporleder*, 666 P.2d at 140)). We have often recognized "that article II, section 7 provides greater privacy protections than the Fourth Amendment," *id.* at ¶ 30, 446 P.3d at 404, and have long rejected the third-party doctrine under that provision of the Colorado Constitution, *e.g.*, *DiGiacomo*, 612 P.2d at 1121; *Sporleder*, 666 P.2d at 143–44. Given the enduring and related privacy concerns presented by a search of an individual's online search history, we see no reason to change course here.

¶31 As the investigators explained in the affidavit, "IP address information can help to identify which computers or other devices were used to access the email account." Once law enforcement has an IP address, it can easily associate that IP address with an individual. *See People v. N.T.B.*, 2019 COA 150, ¶¶ 3–4, 457 P.3d 126, 128–29; *People v. Garrison*, 2017 COA 107, ¶¶ 24–28, 411 P.3d 270, 275–76. Because the IP address provides such a critical link in the chain of user identification, a reasonable expectation of privacy exists at this stage even though law enforcement identified Seymour by name and address only after obtaining a subsequent warrant, which allowed them to see the user profile connected to his IP address.

¶32 Accordingly, we conclude that Seymour has a reasonable expectation of privacy in his Google search history under article II, section 7 of the Colorado Constitution.[6] But Seymour's reasonable expectation of privacy is not the only

[6] Seymour, in his briefing and at oral argument, seems to want to vicariously assert the rights of the many other Google account owners whose privacy interests may have been implicated by law enforcement's conduct here. But "Fourth Amendment rights are personal rights which, like some other constitutional rights, may not be vicariously asserted." *Rakas*, 439 U.S. at 133–34 (quoting *Alderman v. United States*, 394 U.S. 165, 174 (1969)); *see also People v. Sotelo*, 2014 CO 74, ¶ 19, 336 P.3d 188, 191 ("The Fourth Amendment right to be free from unreasonable searches and seizures is a personal right that may not be asserted on another's behalf."). This means that "[t]he fundamental inquiry is 'whether the conduct which the defendant wants to put in issue involved an intrusion into *his* reasonable expectation of privacy.'" *People v. Juarez*, 770 P.2d 1286, 1289 (Colo. 1989) (quoting

potential basis for standing present here; the seizure issue remains. So, we turn there now.

2. The Seizure: A Possessory Interest[7]

¶33 Under both the Fourth Amendment and the Colorado Constitution, a seizure occurs when the government meaningfully interferes with an individual's possessory interests in property. *Hoffman v. People*, 780 P.2d 471, 473 (Colo. 1989); *accord Jacobsen*, 466 U.S. at 113. And several courts have recognized, albeit in different contexts, that individuals can have possessory interests in intangible or digital property. *E.g.*, *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1003 (1984) (holding that, at least for the purposes of the Takings Clause, individuals have property rights in intangible property, such as trade secrets); *Integrated Direct Mktg., LLC v. May*, 495 S.W.3d 73, 76 (Ark. 2016) (holding that electronic data can be converted if a person impedes on the property rights of the owner). Indeed, Google's licensing agreement makes clear that it does not own its users' content. Instead, users own their Google content, which, according to testimony from a Google policy specialist, includes their search histories.

---

4 Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* § 11.3, at 281 (2d ed. 1987)).

[7] When addressing Seymour's *possessory* interest, our opinion is limited to Google accounts and derived from an examination of company-specific policies, terms, and agreements. The discussion on this point should not be taken to address other online search entities, whose user terms may differ from those at issue here.

¶34 "One of the main rights attaching to property is the right to exclude others, and one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of this right to exclude." *Rakas*, 439 U.S. at 143 n.12 (citation omitted). So, while law enforcement can copy digital data without affecting the owner's access to that data, it is the act of copying that meaningfully interferes with the owner's possessory interest because it infringes on one's rights to exclude and to control the dissemination and use of that digital data. *See* Randolph S. Sergent, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 Va. L. Rev. 1181, 1186 (1995); Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 Yale L.J. 700, 710–14 (2010) (discussing that a seizure of digital property occurs when the government copies the data because it is the copying of the digital property rather than control of the physical hardware that preserves it for future evidentiary use and therefore meaningfully interferes with the possessory interest of exclusive control).

¶35 Therefore, law enforcement's copying of Seymour's Google search history meaningfully interfered with his possessory interest in that data and constituted a seizure subject to constitutional protection.[8] This holds true even though, under

[8] These constitutional protections "appl[y] only to those searches [and] seizures conducted by state officials." *People v. Pilkington*, 156 P.3d 477, 479 (Colo. 2007) (quoting *People v. Chastain,* 733 P.2d 1206, 1214 (Colo. 1987)). And state officials can't "circumvent[] the requirements of the fourth amendment by directing a third

the terms of the warrant at issue here, the government initially saw Seymour's Google search history only in connection with an IP address rather than a user identified by name. A trespass is a trespass even if the intruder doesn't know the digital property owner's name. *See Oates*, 698 P.2d at 815–17.

¶36 In sum, law enforcement conducted a search of Seymour's Google activity under the Colorado Constitution and a seizure of that information under both the Colorado Constitution and the Fourth Amendment. Therefore, Seymour has standing to contest the validity of the warrant.

D. First Amendment Materials

¶37 Before addressing whether the warrant here complied with constitutional strictures, we briefly address another constitutional right implicated by these facts: the right to free expression. *See* U.S. Const. amend. I; Colo. Const. art. II, § 10. While neither the federal nor the state constitutional free-speech provisions shield any materials from search or seizure simply because they're expressive, courts must apply the constitutional search-and-seizure requirements with "scrupulous exactitude" when a warrant implicates free speech. *Zurcher*, 436 U.S. at 564

---

party to perform a search that would be improper if the police did it themselves." *Id.* (quoting *Chastain,* 733 P.2d at 1214). Here, although Google employees, rather than law enforcement officers, initially searched the database and copied the relevant data, they did so only in response to the warrant and because law enforcement couldn't access the database directly to conduct the search. Thus, the constitutional protections still apply.

(quoting *Stanford*, 379 U.S. at 485); *see Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1053–55 (Colo. 2002) (concluding this same scrupulous-exactitude standard applies to conflicts between search-and-seizure and free speech rights under the Colorado Constitution). This means that "[w]here presumptively protected materials are sought to be seized, the warrant requirement should be administered to leave as little as possible to the discretion or whim of the officer in the field." *Zurcher*, 436 U.S. at 564.

¶38 The constitutional right to "freedom of speech" protects a panoply of rights, not just the right to speak freely. *Tattered Cover*, 44 P.3d at 1051. Among these are "the right to distribute and sell expressive materials, the right to associate with others, and, most importantly to this case, the right to receive information and ideas." *Id.* Critically, individuals have the right to "engage in expressive activities anonymously, without government intrusion or observation." *Id.* at 1053. Anonymity is vital because individuals may be "chilled" from exercising their rights when expressive activities are publicly disclosed. *Id.* at 1052–53.

¶39 In *Tattered Cover*, we observed that a warrant for an individual's book-purchase record implicated the First Amendment because a bookstore is a place "where a citizen can explore ideas, receive information, and discover myriad perspectives on every topic imaginable." *Id.* at 1052. The internet is used for much the same purpose, and search engines act as gateways to an incomprehensibly vast

library of information. A search term itself may not be sufficiently expressive to receive constitutional protection, but the act of accessing a webpage to receive information—just like purchasing a book—constitutes an expressive activity because the user is seeking to tap into the marketplace of ideas. *See id.* at 1052–53.

¶40 Therefore, we conclude that accessing the internet's marketplace of ideas through a Google search constitutes expressive activity that triggers the need for courts to exercise "scrupulous exactitude" in evaluating the validity of a warrant seeking that search history.[9] With that standard in mind, we now turn to the warrant at issue here.

---

[9] The scope of Seymour's claim under *Tattered Cover* is unclear. *Tattered Cover* addresses how governmental searches under the Fourth Amendment intersect with individuals' free-speech rights under both the First Amendment and article II, section 10 of the Colorado Constitution. *Tattered Cover*, 44 P.3d at 1047. Concluding that the First Amendment failed to adequately safeguard the rights of book buyers and sellers to engage in expressive activity, we held under the Colorado Constitution that "an innocent, third-party bookstore [such as Tattered Cover] must be afforded an opportunity for a hearing prior to the execution of any search warrant that seeks to obtain its customers' book-purchasing records." *Id.* at 1061. At that hearing, the court must balance law enforcement's need for the information against the harm to expressive activity. *Id.* Here, Google sought no such hearing. To the extent that Seymour seeks to independently invoke *Tattered Cover* as a basis for suppression under article II, section 10 of the Colorado Constitution, that issue wasn't preserved below and thus is not ripe for our review now. *See Forgette v. People*, 2023 CO 4, ¶ 21, 524 P.3d 1, 5 ("To preserve an issue for appellate review, a party must make a timely objection on the record, and that objection must be 'specific enough to draw the trial court's attention to the asserted error.'" (citation omitted) (quoting *People v. Tallent*, 2021 CO 68, ¶ 12, 495 P.3d 944, 948)). Even assuming the issue was forfeited and not waived, any error wasn't plain. *See id.* at ¶ 30, 524 P.3d at 7 (explaining that a waiver extinguishes appellate

E. Warrants

¶41 The Fourth Amendment provides that a warrant shall issue only "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV; *see also* Colo. Const. art. II, § 7 ("[N]o warrant to search any place or seize any person or things shall issue without describing the place to be searched, or the person or thing to be seized, as near as may be, nor without probable cause, supported by oath or affirmation reduced to writing."); *People v. Pacheco*, 175 P.3d 91, 94 (Colo. 2006).

¶42 Because law enforcement obtained a warrant here, we must consider whether the warrant (1) described with sufficient particularity both the place to be searched and the things to be seized and (2) demonstrated probable cause.

---

review, but a forfeited error may be reviewed for plain error). Plain error must be obvious to the trial court. *Phillips v. People*, 2019 CO 72, ¶ 39, 443 P.3d 1016, 1027. In *Tattered Cover*, we emphasized that our holding was narrow and considered "only the constitutional protections afforded when law enforcement officials seek to use a search warrant to obtain customer purchase records from a bookstore [and not] the constitutional implications of any other type of government action that implicates expressive rights." 44 P.3d at 1056 n.20. We are unaware of any precedent that has extended *Tattered Cover* to the circumstances with which we are confronted here. Therefore, any error would not have been obvious to the trial court. Moreover, the question presented here doesn't encompass article II, section 10 of the Colorado Constitution.

1. Particularity

¶43 At the suppression hearing, the trial court determined that the warrant was adequately particularized because it sought a very precise and narrow subset of information. We agree.

¶44 A proper warrant ensures that the government's intrusion will be "confined in scope to particularly described evidence relating to a specific crime for which there is demonstrated probable cause." *People v. Roccaforte*, 919 P.2d 799, 802 (Colo. 1996) (quoting *Voss v. Bergsgaard*, 774 F.2d 402, 404 (10th Cir. 1985)). This particularity requirement strives to cabin the government's discretion in examining otherwise private materials by prohibiting "general warrants," which would permit "a general, exploratory rummaging in a person's belongings." *Andresen v. Maryland*, 427 U.S. 463, 480 (1976) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)); *see also People v. Cox*, 2018 CO 88, ¶ 7, 429 P.3d 75, 78–79 (recognizing that the particularity requirement is required and serves the same purpose under both the federal and the state constitution).

a. Place to Be Searched

¶45 Seymour asserts that a reverse-keyword warrant of the sort at issue here is necessarily overbroad because the "place to be searched" is Google's entire database, including every user account. True enough, at least in a broad, technological sense. But when analyzing the legality of a warrant, the "ultimate

touchstone" is reasonableness. *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006); *see also People v. Davis*, 2019 CO 24, ¶ 15, 438 P.3d 266, 269. Here, the scope of the place to be searched strikes us as reasonable when we consider the filter provided by the search parameters set forth in the warrant. Yes, those parameters establish what the government ultimately seized, but, as we discuss further below, they also serve to dramatically reduce the intrusiveness of the search. In this sense, the tech blends search and seizure.

¶46 But let's not immediately look for explanations based on our brave new computerized world. In any context, a warrant doesn't lack particularity simply because it is broad. After all, "the scope of a lawful search is 'defined by the object of the search and the places in which there is probable cause to believe that it may be found.'" *Maryland v. Garrison*, 480 U.S. 79, 84 (1987) (quoting *United States v. Ross*, 456 U.S. 798, 824 (1982)). This means that a warrant authorizing a search of a large area may still be sufficiently particularized if the description of the place to be searched allows an officer, with reasonable effort, to ascertain the place to be searched, *see Steele v. United States*, 267 U.S. 498, 503 (1925), and assures that the search is "conducted in a manner that minimizes unwarranted intrusions upon privacy," *Andresen*, 427 U.S. at 482 n.11.

¶47 Likewise, a search isn't unconstitutional simply because the government, in some lightning-fast, digital sense, very cursorily examines unrelated documents.

See id. Even when a warrant is adequately particularized, "it is certain that some innocuous documents will be examined . . . to determine whether they are, in fact, among those papers authorized to be seized." *Id.* "[T]raditional searches for paper records, like searches for electronic records, have always entailed the exposure of records that are not the objects of the search to at least superficial examination in order to identify and seize those records that are." *United States v. Ulbricht*, 858 F.3d 71, 100 (2d Cir. 2017), *abrogated on other grounds by Carpenter*, 138 S. Ct. at 2217. Such brief examination doesn't turn an adequately particularized search warrant into an unconstitutional general warrant. *Id.*

¶48 Even in applying the particularity requirement with scrupulous exactitude because expressive activity is involved, we are satisfied that the parameters DPD used were reasonable. A computer briefly scanned Google's database looking for the IP addresses of those accounts that had searched a single address within the fifteen days before the alleged arson. Although the database is large, the narrow search terms, the timeframe constraints, and the fact that the initial search was anonymized all served to minimize any invasion of privacy resulting from the search. *See United States v. Place*, 462 U.S. 696, 705–07 (1983) (observing that, because "[t]he intrusion on possessory interests occasioned by a seizure of one's personal effects can vary both in its nature and extent," both "the manner in which information is obtained" and the scope of information obtained—i.e., if it is

limited—can affect whether the government's intrusion violates an individual's constitutional rights). No human, let alone any law enforcement official, saw information falling outside the warrant's narrow search parameters. *Cf. People v. Coke*, 2020 CO 28, ¶¶ 35–37, 461 P.3d 508, 516 (concluding that the warrant was overbroad because it gave the officers "virtually unfettered access" to view the entire contents of the defendant's phone to find the responsive data). There was no rummaging, at least not of the sort that inspired the founders' creation of the Fourth Amendment.

¶49 Thus, the warrant was sufficiently particularized as to the place to be searched. If the search parameters change in a future warrant—for example, to include terms that are more expansive or more intrusive—so too should a court's analysis of particularity.

b. Things to Be Seized

¶50 A warrant is adequately particularized as to the "things to be seized" when it allows an executing officer to "reasonably ascertain and identify the things authorized to be seized," *Roccaforte*, 919 P.2d at 803, with little discretion to decide which records are responsive, *Marron v. United States*, 275 U.S. 192, 196 (1927).

¶51 Here, the warrant made clear that only records containing one of the nine specified keywords were to be seized, and Google turned over no personal information other than the IP addresses corresponding to the accounts responsive

to that query. The executing officer (or, in this case, the Google employee carrying out the search pursuant to the warrant) had virtually no discretion to determine which records were responsive.

¶52 Seymour points out that Google produced a list of sixty-one user searches, even though only five of them exactly matched a keyword listed in the warrant. The other records Google turned over weren't exact matches because they contained other words in addition to the requested keywords. But the mere overproduction of documents doesn't retroactively make a warrant unconstitutional. The government can't control whether an entity properly follows the dictates of a warrant; it can only control the specificity of the warrant it issues. Properly read, the warrant authorized a search for only nine specified keywords. Google may have produced more records than requested, but that issue is for Google and its users to resolve. The warrant was adequately particularized as to the things to be seized.

¶53 But particularity is only half the battle; now we turn to probable cause.

2. Probable Cause

¶54 A warrant is supported by probable cause "when the affidavit in support of the warrant alleges sufficient facts to warrant a person of reasonable caution to believe that . . . evidence of criminal activity is located at the place to be searched." *Henderson v. People*, 879 P.2d 383, 391 (Colo. 1994). This means that law

enforcement's affidavit must establish a nexus between the alleged criminal activity and the place to be searched. *People v. Leftwich*, 869 P.2d 1260, 1268 (Colo. 1994); *see also People v. Green*, 70 P.3d 1213, 1215 (Colo. 2003) (explaining that, although direct evidence establishing the requisite nexus is helpful, it is not required; "[r]ather, the facts alleged in the affidavit, together with reasonable inferences drawn from those facts, may be enough"). It also means the affidavit must provide the magistrate with "a 'substantial basis for . . . conclud[ing]' that a search would uncover evidence of wrongdoing." *Illinois v. Gates*, 462 U.S. 213, 236 (1983) (alteration in original) (quoting *Jones v. United States*, 362 U.S. 257, 271 (1960), *overruled on other grounds by United States v. Salvucci*, 448 U.S. 83 (1980)). Although whether the affidavit established a sufficient nexus to justify the search and whether the magistrate had a substantial basis to issue the warrant are separate inquiries, *see United States v. Leon*, 468 U.S. 897, 915 (1984); *Leftwich*, 869 P.2d at 1270 n.12, both "utilize a reasonableness standard to review the facts in an affidavit," *Leftwich*, 869 P.2d at 1270 n.12. This requires courts to consider "the totality of the facts and circumstances known to the officer at the time of the search." *Henderson*, 879 P.2d at 391. Because probable cause is a "flexible standard," *People v. Winpigler*, 8 P.3d 439, 444 (Colo. 1999), we generally give "great deference" to the magistrate's determination, *Henderson*, 879 P.2d at 391.

¶55 When evaluating probable cause, however, the quantum of evidence is not the only variable at issue. This court has held that the Fourth Amendment requires "any invasion of a person's Fourth Amendment interests [to] be justified . . . by 'specific and articulable facts' directed to *the person* whose interests are to be invaded." *Gutierrez*, 222 P.3d at 943 (emphasis added) (quoting *United States v. Jaramillo*, 25 F.3d 1146, 1151 (2d Cir. 1994)). Such "individualized probable cause" is necessary for each intrusion of an individual's constitutionally protected privacy interest, whether that interest lies in the individual's person or in records held by a third party. *Id.* at 938–39; *see also, e.g.*, *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979) (holding that the Fourth Amendment requires law enforcement to have probable cause before searching an individual in a bar, even if it had already obtained a valid warrant to search the premises and its proprietor).

¶56 In *Gutierrez*, law enforcement obtained a warrant to search the financial records of nearly 5,000 individuals held by a tax preparer. 222 P.3d at 928. The warrant authorized law enforcement to search for and seize records of individuals whose social security and individual tax identification numbers mismatched in their documents, a common indicator of undocumented status. *Id.* at 930–31. Investigators justified the warrant based on an interview with an undocumented defendant charged with identity theft who said that "everyone knows to go to [the preparer] for their taxes." *Id.* at 930. They argued that this statement, along with

other evidence from the tax preparer and the department of revenue, indicated that a search of all the preparer's files would reveal "evidence of identity theft and criminal impersonation." *Id.*

¶57 After executing the warrant and searching each of the 5,000 files, law enforcement discovered that 1,300 had a mismatch. *Id.* at 931. Gutierrez's file was one of the 1,300, and he was later charged with identity theft and criminal impersonation. *Id.* He sought to suppress the evidence, arguing there was no probable cause to search his personal financial records. *Id.*

¶58 We held that the warrant was unconstitutional because it lacked individualized probable cause; no part of the affidavit indicated that Gutierrez's file would contain evidence of criminal activity. *Id.* at 940. In concluding that individualized probable cause was necessary, we reaffirmed that "probable cause may not be analyzed merely in relation to the property or premises searched"; rather, "probable cause must be analyzed in relation to each individual's constitutionally protected interests." *Id.*

¶59 But what occurred in *Gutierrez* is a far cry from what occurred in the case before us now. There, law enforcement officers physically seized and rummaged through all the tax preparer's files, which were organized by client name, looking for certain information. Here, in contrast, a computer searched a massive database—with no law enforcement eyes on any information and no individuals

identified—looking for nothing other than an address. The initial search simply determined whether the database contained any queries for the residential address at issue. The search was not concerned with who may have inquired; it did not seek the identity of any person; and it did not target any individual's documents. It was only after the search yielded responsive data that law enforcement sought to identify individual accounts (i.e., to connect an IP address to an individual). Thus, the search here was arguably one step removed from the search in *Gutierrez*.

¶60 But we need not resolve today whether a search of such data requires probable cause individualized to a single Google account holder because even if we were to conclude that it does, for the reasons explained below, the evidence here would still be admissible under the exclusionary rule's good-faith exception. Therefore, because resolution of this issue doesn't affect the outcome, we simply assume without deciding that the warrant lacked probable cause.

¶61 As a result, we also need not address whether the magistrate had a "substantial basis" to issue the warrant. Despite the deference to which the magistrate's judgment is entitled and the level of detail in the affidavit supporting the warrant, the core premise of the affidavit is at least debatable, particularly when examined with the scrupulous exactitude required when the government intrudes on an individual's expressive activity. The filing detective asserted, in essence, that someone targeting the house would have digitally cased it, or at least

sought directions, beforehand. Perhaps. But people search addresses for much more innocuous reasons all the time. And if the perpetrators were targeting the victims, one might assume that they were sufficiently familiar with them to dispense with searching the address. Even so, it doesn't matter. Our conclusion as to good faith renders the issue moot.

F. The Good-Faith Exception to the Exclusionary Rule

¶62 Ordinarily, the exclusionary rule requires courts to suppress evidence at trial if the government acquired it in violation of constitutional protections. *See Gutierrez*, 222 P.3d at 941 (considering the exclusionary rule under the Fourth Amendment); *McKnight*, ¶ 61, 446 P.3d at 413–14 (same under the Colorado Constitution). The purpose of the rule is to deter police misconduct. *Michigan v. Tucker*, 417 U.S. 433, 447 (1974). When applied, the exclusionary rule "necessarily assumes that the police have engaged in willful, or at the very least negligent, conduct which has deprived the defendant of some right." *Id.*

¶63 The good-faith exception to the exclusionary rule provides that "evidence obtained in violation of the Fourth Amendment should not be suppressed in circumstances where the evidence was obtained by officers acting in objectively reasonable reliance on a warrant issued by a detached and neutral magistrate, even if that warrant was later determined to be invalid." *Gutierrez,* 222 P.3d at 941; *see also Leftwich*, 869 P.2d at 1272 (holding that Colorado's good-faith exception,

codified in section 16-3-308, C.R.S. (2023), is "substantially similar" to the Supreme Court's rule). The exception exists because there is little chance suppression will deter police misconduct in cases where the police didn't know their conduct was illegal in the first place. *Leon*, 468 U.S. at 918–19. In such cases, "the social costs of suppression would outweigh any possible deterrent effect." *Gutierrez*, 222 P.3d at 941.

¶64 The parties here do not dispute that the warrant was issued by a detached and neutral magistrate, so the issue is whether investigators' reliance on the warrant was objectively reasonable. *See Pacheco*, 175 P.3d at 96 ("The test for good faith is 'whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization,' taking into account all of the circumstances surrounding the issuance of the warrant." (quoting *Leon,* 468 U.S. at 922 n.23)). We have recognized only four circumstances that will render an officer's reliance on a warrant unreasonable:

> (1) where the issuing magistrate was misled by a known or recklessly made falsehood; (2) where the issuing magistrate wholly abandoned the judicial role; (3) where the warrant is so facially deficient that the officer cannot reasonably determine the particular place to be searched or things to be seized; or (4) where the warrant is based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.

People v. Miller, 75 P.3d 1108, 1114 (Colo. 2003).

¶65 Seymour argues that the good-faith exception should not apply here for primarily two reasons. First, he argues that investigators misled the magistrate by failing to reveal that the search would violate the privacy of *all* Google users. By extension, he also argues that the warrant was so facially deficient in particularity that officers wouldn't be able to identify the place to be searched or the things to be seized. But, having already concluded that the warrant was sufficiently particularized and that it didn't, therefore, authorize an unreasonable search of all Google users, we disagree.

¶66 Second, Seymour contends that exclusion is appropriate because the warrant was based on an allegedly "bare bones" affidavit, which was "so lacking in indicia of probable cause" that it was unreasonable for an officer to rely on it. *Leon*, 468 U.S. at 923 (quoting *Brown v. Illinois*, 422 U.S. 590, 611 (1975) (Powell, J., concurring in part)); *accord People v. Altman*, 960 P.2d 1164, 1169 (Colo. 1998).

¶67 An affidavit is bare bones when it fails to establish a "minimally sufficient nexus between the illegal activity and the place to be searched." *Gutierrez*, 222 P.3d at 941 (quoting *United States v. Carpenter*, 360 F.3d 591, 596 (6th Cir. 2004)). However, an affidavit is not bare bones simply because it failed to establish a "substantial basis" for a magistrate to issue a warrant. *Leon*, 468 U.S. at 915. "Police officers are not appellate judges." *Altman*, 960 P.2d at 1170; *see also Gutierrez*, 222 P.3d at 942 (noting that the term "'objectively reasonable' may have

one meaning when applied to magistrates and another when applied to police officers"); *Leftwich*, 869 P.2d at 1270 n.12. Thus, an officer may reasonably rely on what is later determined to be an invalid warrant when the affidavit supporting the warrant establishes at least a "minimally sufficient nexus." *Cf. Gutierrez*, 222 P.3d at 941.

¶68 Seymour relies on *Gutierrez*, where we concluded that the warrant was bare bones because it failed to establish a nexus between the alleged crime and the defendant's financial record such that "no reasonably well-trained officer could rely upon it." 222 P.3d at 943–44. By extension, Seymour argues that the affidavit here was bare bones because it necessarily lacked a nexus between his specific Google account and the alleged arson, given that it lacked any identifying information related to him at all.

¶69 But the good-faith analysis in *Gutierrez* is distinguishable. True, we held there that the good-faith exception did not apply, but we had already recognized that individuals have a reasonable expectation of privacy in their financial records when *Gutierrez* was decided. *Id.* at 933 (citing numerous cases and statutes establishing that an individual's financial records are protected under Colorado law). So, the police were on notice that a nexus was required between a crime and Gutierrez's individual tax records. *See id.*

¶70 By contrast, until today, no court had established that individuals have a constitutionally protected privacy interest in their Google search history. *Cf. Commonwealth v. Kurtz,* 294 A.3d 509, 522 (Pa. Super. Ct. 2023) (holding that, under the third-party doctrine, the defendant did not have a reasonable expectation of privacy in his search history). In the absence of precedent explicitly establishing that an individual's Google search history is constitutionally protected, DPD had no reason to know that it might have needed to demonstrate a connection between the alleged crime and Seymour's individual Google account. *See People v. Corr*, 682 P.2d 20, 27–28 (Colo. 1984); *cf. Davis v. United States*, 564 U.S. 229, 232 (2011) (holding that "searches conducted in objectively reasonable reliance on binding appellate precedent are not subject to the exclusionary rule").

¶71 In the absence of precedent requiring individualized probable cause in this context, DPD reasonably believed it only needed to show a nexus between the alleged crime and a subset of Google's database. In an eight-page affidavit—which the reviewing judge called one of the most detailed he had seen in a long time—the affiant explained why, based on his training and experience, he believed the fire had been planned; why he believed the perpetrators searched the address online beforehand; and why the record of that search could be found in Google's database. To the extent investigators reasonably believed it was legally necessary, the affidavit demonstrated the requisite minimum nexus between the alleged

arson and Google's database. *See Altman*, 960 P.2d at 1170–72 (recognizing that, because "probable cause deals with probabilities, not certainties," an officer's objectively reasonable belief that an affidavit contains a sufficient nexus to support a probable-cause finding may be based in part on his experience and training in evaluating noncriminal activities and otherwise-innocent facts).[10]

¶72 We agree with the trial court that the deterrent purpose of the exclusionary rule would not be served by suppressing evidence from a warrant—several iterations of which were approved by two judges—that authorized a relatively new and previously unchallenged investigative technique. At every step, law enforcement acted reasonably to carry out a novel search in a constitutional manner. Suppressing the evidence here wouldn't deter police misconduct. Thus, we conclude the good-faith exception applies.

III. Conclusion

¶73 We discharge the rule to show cause and remand the case to the trial court for further proceedings consistent with this opinion.

---

[10] The government's compliance with this minimal-nexus requirement here obviously serves to distinguish this case from others involving reverse-keyword warrants authorizing searches for addresses involving *no* nexus to suspected criminal activity. For example, the government may not use a warrant to see who has "Googled" the address of a place of worship, a doctor's office, or any other place where individuals might engage in intensely personal activity without the address being connected to a crime. If there was no crime at the address in question, there is no potential nexus. The same holds true for any other keyword.

JUSTICE BERKENKOTTER concurred in the judgment.

JUSTICE MÁRQUEZ, joined by **JUSTICE SAMOUR**, dissented.

JUSTICE BERKENKOTTER concurring in the judgment.

¶74 I agree with the dissent that the search here was unconstitutional.

¶75 Specifically, I agree that Seymour and each of the billion Google users across the globe had privacy and possessory interests in their internet search records, and thus both the Fourth Amendment and article II, section 7 of the Colorado Constitution required the Denver Police Department to have individualized probable cause with respect to each of the users before it could direct Google to search those records for the Department. Dis. op. ¶¶ 19–20, 28. Here, there was no probable cause as to any individual Google user. Certainly, there was no probable cause as to Seymour.

¶76 And like the dissent, I strongly disagree with the majority's conclusion that the examination of a billion Google users' search histories was not unreasonably intrusive because the government didn't ultimately seize all of those search histories. Dis. op. ¶ 24. This conclusion implies that a reverse-keyword warrant merits a different kind of Fourth Amendment analysis because "tech blends search and seizure." Maj. op. ¶ 45. To my mind, this turns Fourth Amendment jurisprudence on its head as it suggests that an absolute lack of particularity as to the place to be searched can be overcome so long as a warrant is sufficiently specific regarding the thing to be seized. The problem with this reasoning, as the dissent observes, is that it fundamentally conflates the place to be searched (a

billion users' specific internet search queries) with the things to be seized (the keyword search results). Dis. op. ¶¶ 34–35. In so doing, the majority essentially creates a special rule for reverse-keyword warrants that collapses both parts of the Fourth Amendment's particularity test into a test based solely on the description of the thing to be seized.

¶77 That is, for the majority, tech seems not to have *blended* search and seizure so much as it has *blurred* search and seizure.[1]

¶78 But I write separately to concur in the judgment because, like the majority, I conclude that the evidence obtained through the two warrants is insulated by the good-faith exception to the exclusionary rule. I reach this conclusion for essentially the same reason as the majority: There is no well-established law in Colorado—or anywhere else, for that matter—concerning the constitutionality of reverse-keyword searches. The Denver Police Department had no reason to know that individuals have a constitutionally protected interest in their Google search history or that the Department might have needed to demonstrate a connection between the alleged crime and Seymour's individual Google account. Maj. op. ¶ 70. Under these circumstances, I conclude that the officers acted reasonably in

[1] I am also concerned that the majority's reasoning throughout its opinion rests on a somewhat fuzzy understanding of the technology at play in this case and others that raise questions about the boundaries of the Fourth Amendment.

carrying out this novel type of search. Here, their reliance on the warrants was objectively reasonable, though in my view, going forward, that would not be so.

¶79 This is why, even though I agree with the dissent's analysis and its conclusion that the reverse-keyword search warrant was invalid, I would discharge the rule to show cause.

JUSTICE MÁRQUEZ, joined by JUSTICE SAMOUR, dissenting.

¶80 Today, the court blesses law enforcement's use of a powerful new tool of the digital age: the reverse-keyword warrant. To be sure, law enforcement searches for electronic information are nothing new. These days, instead of searching a person's "papers and effects" sitting in a box, desk, or filing cabinet, police might instead obtain a warrant to search the contents of a person's cell phone or laptop. As we know, such electronic devices "not only contain[] in digital form many sensitive records previously found in the home," but also "a broad array of private information never found in a home in any form," including "[i]nternet search and browsing history" that can "reveal an individual's private interests or concerns." *Riley v. California*, 573 U.S. 373, 395–97 (2014).

¶81 Under a traditional warrant for electronic information, law enforcement must have probable cause to search a specific user account or electronic device (e.g., a particular cell phone or laptop). Such warrants are used to search for specific digital evidence relating to a crime committed by a known suspect. By contrast, a reverse-keyword warrant functions like a digital dragnet. Police officers relying on reverse-keyword warrants don't have an identified suspect. Instead—as in this case—they surmise that the perpetrator might have searched the internet for something related to the crime. Maj. op. ¶ 7. So, they direct a search engine company, like Google, to scan its entire collection of user

data—here, the search histories of a billion users worldwide—and, based on that scan, to identify the IP address of every user who searched the internet using particular keywords or phrases the police deem relevant to their investigation.

¶82 Let that sink in for a moment. The basic purpose of the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018) (quoting *Camara v. Mun. Ct. of S.F.*, 387 U.S. 523, 528 (1967)). But by authorizing law enforcement to rummage through the private search histories of a billion individuals for potential evidence of criminal activity, reverse-keyword warrants permit exactly what the Fourth Amendment forbids. They are tantamount to a high-tech version of the reviled "general warrants" that first gave rise to the protections in the Fourth Amendment. *See* Maj. op. ¶ 44.

¶83 The majority holds that "Seymour has a reasonable expectation of privacy in his Google search history," *id.* at ¶ 32, and that law enforcement "meaningfully interfered with [Seymour's] possessory interest" in his Google search history, resulting in "a seizure of that information under both the Fourth Amendment and the Colorado Constitution," *id.* at ¶¶ 35–36. I agree. I further agree that a person's search history can implicate constitutional freedom of expression, which means that the Fourth Amendment's protections must be applied with "scrupulous exactitude." *Id.* at ¶¶ 3, 40 (quoting *Zurcher v. Stanford Daily*, 436 U.S. 547, 564

(1978)). But unlike the majority, I would follow these aspects of the majority's reasoning to their logical conclusion: the warrant here was invalid under both the Fourth Amendment and article II, section 7 of the Colorado Constitution, and the good-faith exception to the exclusionary rule cannot salvage its unconstitutionality.

¶84 First, to determine the validity of the warrant—which is the overarching issue here—we must identify the search or seizure the warrant authorized. The majority holds that law enforcement "conducted a search of Seymour's Google activity under the Colorado Constitution and a seizure of that information under both the Fourth Amendment and the Colorado Constitution." *Id.* at ¶ 36. That's right. But the activity the warrant authorized also constituted a "search" under the Fourth Amendment. The majority's reluctance to reach this conclusion stems, in part, from its failure to analyze the first activity the warrant authorized: the scan of Google's entire database of user accounts.

¶85 If, as the majority acknowledges, Seymour has both privacy and possessory interests in his Google search history, *id.* at ¶¶ 26–27, 35, then so does every other Google user. And if every Google user has privacy and possessory interests in their search history, then a government-directed scan of a billion such histories necessarily intrudes upon those collective interests. Such a scan, therefore,

constitutes a "search" within the meaning of the Fourth Amendment—not merely with respect to Seymour's data, but rather with respect to *all* user data scanned.

¶86 Initially, the majority tries to sidestep this conclusion; first, by looking to inapposite federal cases applying the third-party doctrine to IP addresses, *id.* at ¶¶ 28–29, and then by erroneously suggesting that Seymour seeks to vicariously assert the Fourth Amendment rights of others not before this court, *id.* at ¶ 32 n.6. Yet later, the majority shifts its focus back to Google users' search histories and all but concedes the point. *Id.* at ¶ 45 (describing the "place to be searched" as "Google's entire database, including every user account"); *see also id.* at ¶ 48 ("A computer briefly scanned Google's database . . . ."). I would avoid this tension and simply follow the majority's own analysis of Seymour's privacy and possessory interests: the initial scan of Google's entire database constituted a Fourth Amendment "search."

¶87 Second, because Seymour (and every other Google user) has privacy and possessory interests in their search histories, both the Fourth Amendment and article II, section 7 of the Colorado Constitution require law enforcement to have probable cause to scan an individual user's search history. *See People v. Gutierrez*, 222 P.3d 925, 938 (Colo. 2009). But in this case, law enforcement employed a reverse-keyword search precisely because it *lacked* probable cause with respect to *any* individual Google user associated with an IP address—let alone Seymour.

Indeed, law enforcement admitted to having no more than a "hunch" that a digital fishing expedition through Google's entire collection of individuals' private information might yield results where lawful investigative techniques had failed. We know, however, that "[a]n officer's hunch" is insufficient to establish probable cause. *People v. Smith*, 2022 CO 38, ¶ 33, 511 P.3d 647, 654. So, it is puzzling for the majority to hedge and simply "assume without deciding that the warrant lacked probable cause." Maj. op. ¶ 60. The lack of probable cause is apparent on the face of the warrant.

¶88 Third, law enforcement's lack of probable cause with respect to any individual Google account only underscores the lack of particularity with which the warrant described the place to be searched. Importantly, "the scope of a lawful search is 'defined by the object of the search and the *places in which there is probable cause* to believe that it may be found.'" *Maryland v. Garrison*, 480 U.S. 79, 84 (1987) (emphasis added) (quoting *United States v. Ross*, 456 U.S. 798, 824 (1982)). Here, law enforcement officers had no idea *where* to look for the specific records they were seeking because they had no idea which—*if any*—user accounts might contain search histories that included the identified keywords. The complete absence of probable cause as to any individual Google account logically forecloses the conclusion that the warrant was sufficiently particularized with respect to the place to be searched (Google's entire database of a *billion* user accounts). To escape

this conclusion, the majority relies on the purportedly "narrow" search parameters that, according to the majority, limit the place to be searched by the specificity of the data to be seized (i.e., the IP addresses of those users who searched for designated keywords within a specific timeframe). Maj. op. ¶¶ 45, 48. But relying on the information seized to somehow define the place that was searched (a billion user accounts) defies logic and conflates distinct constitutional requirements. Such an approach impermissibly justifies a government search of literally *any* location where the sought-after evidence might be found. *United States v. Alberts*, 721 F.2d 636, 639 (8th Cir. 1983) (rejecting the notion that garbage bags to be seized pursuant to a warrant also constituted the place to be searched because, were that true, "the officers would have been justified in searching anywhere that the bags conceivably might have been located"); *see also* 2 Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* § 4.5, Westlaw (database updated Oct. 2022) (citing *Alberts* for this proposition).

¶89 Fourth, the warrant was so facially deficient that it forecloses application of the good-faith exception to the exclusionary rule. As the majority admits, the warrant was not based on individualized probable cause with respect to any Google user. *See* Maj. op. ¶¶ 59–61. Yet, precisely for this reason, the warrant lacked sufficient particularity with regard to the place to be searched. Under these

circumstances, law enforcement should have "be[en] aware that [its] endeavor was essentially a fishing expedition." *Gutierrez*, 222 P.3d at 944.

¶90 The technology used in this case "risks Government encroachment of the sort the Framers . . . drafted the Fourth Amendment to prevent." *Carpenter*, 138 S. Ct. at 2223. The majority, however, fails to apply the "longstanding Fourth Amendment constitutional protections" this technology demands, *In re Search of: Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 756 (N.D. Ill. 2020), and instead, permits law enforcement to bypass Fourth Amendment protections through novel technological means. Although law enforcement turned to this option because other, constitutional methods proved fruitless, Maj. op. ¶¶ 6–7, after today's decision, I anticipate that reverse-keyword warrants will swiftly become the investigative tool of first resort. Because, why not? It's a tantalizingly easy shortcut to generating a list of potential suspects. *See* Julia Love & Davey Alba, *Google User Data Has Become a Favorite Police Shortcut*, Bloomberg Businessweek (Sept. 27, 2023).

¶91 I cannot join today's ruling. The privacy the Framers cherished "comes at a cost," and the United States Supreme Court has recognized that Fourth Amendment protections must be respected, even when doing so "will have an impact on the ability of law enforcement to combat crime." *Riley*, 573 U.S. at 401.

Because we cannot ignore these constitutional protections, even when law enforcement hits an investigative dead end, I respectfully dissent.

IV. The Nature of Reverse-Keyword Warrants

¶92 The scale of a reverse-keyword search is staggering. "By their nature, reverse keyword searches allow law enforcement to obtain information about every single person searching for specific terms," or keywords, that law enforcement selects. Brief for Elec. Priv. Info. Ctr. as Amicus Curiae Supporting Defendant, at 5–6. In Google's case, this means that, when law enforcement so directs, Google scans the histories of its approximately one-billion users to identify which of those histories, if any, contain records of searches for those keywords within a specific timeframe.

¶93 Keywords are not innocuous data. People routinely type keywords into a search engine (most likely Google) to navigate the internet: to access controversial ideas; to answer medical questions; or, indeed, to obtain directions to a particular address. Brief for Elec. Frontier Found. as Amicus Curiae Supporting Defendant ("Elec. Frontier Found. Brief"), at 6. Therefore, the keywords that constitute "[a]n [i]nternet search and browsing history . . . could reveal an individual's private interests or concerns" to law enforcement.[1] *Riley*, 573 U.S. at 395. And because

[1] For related reasons, the majority concludes—and I agree—that such searches can implicate an individual's rights under the First Amendment and corresponding

every keyword search is linked to the user who performed it, Elec. Frontier Found. Brief, at 9–10, reverse-keyword searches give law enforcement unprecedented access to individuals' digitized thoughts.

¶94 Unlike typical warrants for electronic information authorizing the search of a particular suspect's phone or laptop, reverse-keyword searches are "not targeted to specific individuals or accounts." *Id.* at 3. To the contrary, "the police generally have no identified suspects when they seek a keyword search warrant." *Id.* Indeed, "the sole basis for" such a warrant is "the officer's hunch that the suspect," whoever they may be, "might have searched for something related to the crime." *Id.*

¶95 Based on that hunch, law enforcement directs a search engine like Google to rummage through each of Google's billion user accounts and identify the IP

---

rights under article II, section 10 of the Colorado Constitution. Maj. op. ¶¶ 37–40. But if anything, the notion that the Fourth Amendment must be applied with "scrupulous exactitude" when law enforcement seeks to seize materials that implicate the First Amendment, *Zurcher*, 436 U.S. at 564 (quoting *Stanford v. Texas*, 379 U.S. 476, 485 (1965)), only further undermines the majority's analysis of the warrant here. Moreover, because I conclude that the warrant failed to meet Fourth Amendment requirements, I see no reason to address Seymour's claim under *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044 (Colo. 2002). *Tattered Cover* discussed additional protections "*beyond* the general Fourth Amendment requirements applicable to all warrants" when law enforcement seeks to seize expressive materials. *Id.* at 1055 (emphasis added). We need not examine whether the warrant ran afoul of those additional protections where, as here, the warrant failed to meet traditional Fourth Amendment requirements.

addresses of those users who entered specific keywords during a particular timeframe. The government uses this digital dragnet to snare a pool of potential suspects without having probable cause to search or seize *any* individual user's search history—let alone the private search histories of the users caught in the dragnet, including those of plainly innocent individuals. Here, for example, the record shows that law enforcement's search and seizure of private digital data captured the search histories of two people officers quickly ruled out as suspects, plus information from three other accounts outside Colorado. *See* Maj. op. ¶ 12.

V. Scanning Google's Database Constitutes a "Search"

¶96 The majority, like other courts that have considered comparable search warrants,[2] skips the step of analyzing whether the scan of Google's database of user accounts constituted a "search" within the meaning of the Fourth Amendment. *See, e.g.*, *In re Search of: Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 740 (assuming without deciding that a geofence constitutes a

[2] Geofence warrants, for example, are used by law enforcement to identify individuals who were in a certain area at a certain time. Similar to a reverse-keyword warrant, a geofence warrant requires Google to scan its *entire* database—in those cases, for users' location history data. *United States v. Chatrie*, 590 F. Supp. 3d 901, 914–15 (E.D. Va. 2022). Geofence warrants thus provide law enforcement "an almost unlimited pool from which to seek location data" that inevitably reveals the private activities of many innocent individuals. *Id.* at 925–26. The "pool" of data available to law enforcement when using a reverse-keyword warrant is similarly vast, as Google must search its entire database of user accounts to return the information sought.

search); *see also United States v. Chatrie*, 590 F. Supp. 3d 901, 929–33 (E.D. Va. 2022) (holding a geofence warrant invalid on grounds that it lacked particularized probable cause to search each Google user within the geofence); Note, *Geofence Warrants and the Fourth Amendment*, 134 Harv. L. Rev. 2508, 2515 (2021) ("[M]ost [courts] have implicitly treated the search as the point when the private company [e.g., Google] first provides law enforcement with the data requested . . . with no explanation why."). But because a warrant defines the lawful scope of a Fourth Amendment "search," *Kentucky v. King*, 563 U.S. 452, 459 (2011), it is critical to identify the search conducted under that warrant's authority in order to properly analyze the validity of the warrant.

¶97 A "search" within the meaning of the Fourth Amendment occurs when the government either (1) "obtains information by physically intruding on a constitutionally protected area," *United States v. Jones*, 565 U.S. 400, 406 n.3 (2012), (the "property-based" theory); or (2) "violates a subjective expectation of privacy that society recognizes as reasonable," *Kyllo v. United States*, 533 U.S. 27, 33 (2001) (citing *Katz v. United States*, 389 U.S. 347, 361 (1967)), (the "privacy-based" theory).

¶98 First, under the property-based theory of the Fourth Amendment, the government performs a search when it "physically occupie[s] private property for the purpose of obtaining information." *Jones*, 565 U.S. at 404–05; *see also id.* at 414 (Sotomayor, J., concurring) ("When the government physically invades personal

property to gather information, a search occurs."). As the majority acknowledges, several courts have recognized that individuals can have "possessory interests in intangible or digital property." Maj. op. ¶ 33 (citing *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1003 (1984); *Integrated Direct Mktg., LLC v. May*, 495 S.W.3d 73, 76 (Ark. 2016)). The United States Supreme Court shares this view. *See Carpenter*, 138 S. Ct. at 2222 (suggesting a detailed log of a person's location derived from cell site location data constitutes the "modern-day equivalent" of an individual's "papers" or "effects"). Because "the hallmark of any search" is "the fact of the intrusion into a closed area otherwise hidden from human view," *People v. McKnight*, 2019 CO 36, ¶ 46, 446 P.3d 397, 409 (quoting *United States v. Bronstein*, 521 F.2d 459, 464 (2d Cir. 1975) (Mansfield, J., concurring)), the government-directed scan of Seymour's Google search history for particular keywords constituted a Fourth Amendment "search." In other words, law enforcement's digital entry into Seymour's search history constituted a trespass on his digital property.[3]

---

[3] The majority inaccurately suggests that possessory interests are relevant only to whether a seizure has occurred. Maj. op. ¶¶ 20, 34–35. Although I agree that the copying of Seymour's data amounted to a trespass for purposes of effectuating a Fourth Amendment *seizure* of that information, *id.* at ¶¶ 34–35, the United States Supreme Court has expressly held that when "the Government obtains information by physically intruding on a constitutionally protected area," a "search" under the Fourth Amendment "has undoubtedly occurred," *Jones*, 565 U.S. at 406 n.3 (2012); *see also People v. Oates*, 698 P.2d 811, 817 (Colo. 1985)

¶99 Second, under the privacy-based theory of the Fourth Amendment, "[w]hen an individual 'seeks to preserve something as private,' and [their] expectation of privacy is 'one that society is prepared to recognize as reasonable,' . . . official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause." *Carpenter*, 138 S. Ct. at 2213 (quoting *Smith v. Maryland*, 442 U.S. 735, 740 (1979)). As the majority recognizes, "[t]he contents of an individual's internet searches reveal as much, if not in many instances more about one's private life" than the location data discussed in *Carpenter*. Maj. op. ¶ 26. The majority thus holds, and I agree, that Seymour has a reasonable expectation of privacy in his Google search history. *Id.* at ¶ 31. But this necessarily means that every Google user has the same reasonable expectation of privacy in their search history. It also means that scanning the search histories of a billion Google users for particular keywords intrudes on that privacy interest and constitutes a search—under *both* the Fourth Amendment *and* the Colorado Constitution.

¶100 Curiously, the majority limits its holding to the Colorado Constitution, reasoning that the federal third-party doctrine would lead to a different result

---

("government entry . . . into places concealed from public view" is also the kind of trespass that constitutes a *search* and, therefore, may violate an individual's Fourth Amendment rights).

under the Fourth Amendment. *Id.* at ¶¶ 29–32. But the third-party doctrine cases it cites are distinguishable. Those cases concern searches for IP address data relating to a single suspect; they also distinguish such data from the location data at issue in *Carpenter*. *See United States v. Rosenow*, 50 F.4th 715, 737–38 (9th Cir. 2022) (observing that IP address data "is provided to and used by Internet service providers for the specific purpose of directing the routing of information"); *United States v. Hood*, 920 F.3d 87, 89, 92 (1st Cir. 2019) (noting that IP address data is generated through an individual's "affirmative decision to access a website or application" and does not reveal private information); *United States v. Soybel*, 13 F.4th 584, 593 (7th Cir. 2021) (observing that IP pen registers generate limited, non-retrospective location data and do not "intercept the content of [an individual's] communications"); *cf. Heeger v. Facebook, Inc.*, 509 F. Supp. 3d 1182, 1189–90 (N.D. Cal. 2020) (distinguishing the data at issue in *Carpenter* from IP addresses for purposes of standing under Article III of the federal constitution, not the Fourth Amendment).

¶101 Federal cases involving geofence warrants—which are far more analogous to reverse-keyword searches—suggest that *Carpenter*'s limits on the third-party doctrine apply with equal force—even where the data those warrants return is anonymized. *United States v. Rhine*, No. CR 21-0687 (RC), 2023 WL 372044, at *27–28 (D.D.C. Jan. 24, 2023); *Chatrie*, 590 F. Supp. 3d at 915–16, 935–36; *In re Search*

of: Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d at 736–37. Courts in those cases focused on the vast scope of private information that location data could reveal. Similarly, here, a person's Google history reveals the "privacies of life"—a concern the majority readily acknowledges. Maj. op. ¶¶ 24–27. Thus, when law enforcement rummaged through the Google search histories of Seymour—and a billion others—it violated their reasonable expectations of privacy, *id.* at ¶ 32, and performed a "search" within the meaning of the Fourth Amendment.[4]

¶102 The majority further undermines its own conclusion when it suggests that Seymour seeks inappropriately to raise the Fourth Amendment rights of others not before the court. *See id.* at ¶ 32 n.6. Here, the majority misunderstands Seymour's argument. In determining whether a Fourth Amendment "search" has occurred, courts must ask if "the police intrude[d] upon *anyone's* justified expectation of privacy." 6 LaFave, *supra*, § 11.3 (emphasis added). Here, Seymour's references to the rights of other Google users address this question and serve simply to illustrate the breadth of the search the warrant authorized. Whether Seymour lacks standing to assert the rights of other Google users neither

[4] In any event, the majority's discussion of the third-party doctrine is superfluous, given that the majority ultimately concludes that the seizure of Seymour's digital data violated his *possessory* interests under the Fourth Amendment. Maj. op. ¶ 36.

undermines Seymour's standing to assert his own rights nor forecloses an analysis of whether the initial scan constituted a Fourth Amendment search.

¶103 Seymour's point is, if he has a reasonable expectation of privacy in his Google search history, then so does every other Google user. Law enforcement treated Seymour's information no differently than it treated the information of every other Google user; it rummaged through the private search histories of all billion Google users (including Seymour) in the hope of finding accounts linked to particular search terms in a specific timeframe. Under either the property- or the privacy-based theory, such conduct amounts to a search under the Fourth Amendment.

¶104 Keep in mind that, even under the majority's narrow view of the search here, law enforcement's dragnet ensnared two people officers easily ruled out as suspects, not to mention three additional accounts from outside Colorado. *Id.* at ¶ 12. In other words, the reverse-keyword search here implicated others' rights—whether a billion others under my approach, or a handful under the majority's. When law enforcement intrusion implicates the Fourth Amendment rights of *anyone*, law enforcement performs a Fourth Amendment "search." 6 LaFave, *supra*, § 11.3.

¶105 In sum, I conclude that the initial scan involved in reverse-keyword searches constitutes a Fourth Amendment "search" of the user accounts scanned. I therefore analyze the validity of the warrant here with its true scope in mind.

VI. The Warrant Did Not Satisfy Constitutional Requirements

¶106 Because the warrant here was not supported by probable cause and lacked particularity as to the place to be searched, it does not pass constitutional muster.

A. Probable Cause

¶107 Probable cause demands a reasonable ground for belief of guilt with respect to "each individual's constitutionally protected interests." *Gutierrez*, 222 P.3d at 938. The majority correctly holds that individuals have a protected interest in their Google search histories, at least under the Colorado Constitution. Maj. op. ¶ 32. Here, however, the affidavit supporting the warrant included no information to justify a search of Seymour's individual account—or of any individual Google user's account, for that matter. During the suppression hearing, the investigating officer conceded that the police lacked probable cause to search Seymour's account; indeed, he testified the reverse-keyword warrant was based on no more than a "hunch" that the perpetrator may have searched for the address where the arson occurred. Yet it is well-established that "a mere generalized suspicion or hunch" is not enough to establish reasonable suspicion, *People v. Wheeler*, 2020 CO 65, ¶ 13, 465 P.3d 47, 52—let alone the considerably more demanding level of proof

required for probable cause, *Kansas v. Glover*, 140 S. Ct. 1183, 1187 (2020) (citing *Prado Navarette v. California*, 572 U.S. 393, 397 (2014)). Consequently, the warrant here plainly was not supported by probable cause; yet, the majority is reluctant to hold this. I see no reason for such evasion.

¶108 Our decision in *Gutierrez* is dispositive here. In that case, the warrant authorized an "unbridled search" of 5,000 tax files based on law enforcement's theory that it might find evidence of criminal activity. We held that such a warrant lacked the requisite probable cause to authorize a search of Gutierrez's individual file. *Gutierrez*, 222 P.3d at 929, 930, 940. In reaching that conclusion, we squarely rejected the notion that law enforcement's belief that *some* files among a collection of thousands might contain evidence of criminal activity was sufficient to establish probable cause when officers had no reason to suspect any particular file over another. *Id.* Indeed, we reasoned that the fact that only 1,300 of the 5,000 files searched were found to contain evidence of wrongdoing only "highlight[ed] the absence of any nexus between the particular tax returns searched and criminal activity." *Id.* at 943–44.

¶109 This case is even more stark. Here, law enforcement hypothesized that the perpetrator might have used Google to search the address where the arson occurred. The affidavit containing this hypothesis was based on the "at least debatable" premise, as the majority describes it, that if the home was specifically

targeted, the perpetrator would have searched its address. Maj. op. ¶ 61. Nowhere did the affidavit name Seymour—or anyone else, for that matter—as a potential suspect. Absent particularized probable cause, the warrant at issue authorized a wholly "'exploratory search' designed to . . . rummage through the 'confidential records'" of a billion Google users "based on nothing more than a suspicion that one or more of them," never mind who, "may have committed a crime." *Gutierrez*, 222 P.3d at 931. As in *Gutierrez*, the limited number of "hits" that resulted from this global search only underscores "the absence of any nexus between the [billion Google user accounts] searched and criminal activity." *Id.* at 943–44.

¶110 In the majority's view, individualized probable cause may not have been necessary in this case at all because the initial scan of Google's database returned records of search queries without "target[ing] any individual's documents." Maj. op. ¶ 59. But this is precisely the reason we characterized the warrant in *Gutierrez* as "essentially a fishing expedition." 222 P.3d at 944. And to the extent that the majority distinguishes *Gutierrez* because there, law enforcement saw client names rather than users' IP addresses, Maj. op. ¶ 59, the majority contradicts itself yet again. As the majority recognizes, IP addresses provide a "critical link in the chain of user identification" sufficient to create a reasonable expectation of privacy, even before law enforcement has performed the "eas[y]" task of

"associat[ing] that IP address with an individual."[5] *Id.* at ¶ 31. It therefore makes little sense for the majority to turn around and rely on the same (short) distance between an IP address and a name to suggest that the search here may not have required individualized probable cause.

¶111 The majority also distinguishes *Gutierrez* on grounds that it involved the *physical* search and seizure of client files rather than a *digital* scan of comparable files. *Id.* at ¶ 59. But this logic implies that law enforcement's unlawful rummaging through the 5,000 files in *Gutierrez* would be constitutional if those same files were electronic, and the means of searching them digital instead of human. Not so. The fact that a reverse-keyword search swiftly facilitates such "general, exploratory rummaging," *Andresen v. Maryland*, 427 U.S. 463, 480 (1976) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)), via digital means (rather than old-fashioned police legwork) only reinforces the need to protect the

[5] The majority appears to limit this aspect of its discussion of IP addresses to a state constitutional analysis. Maj. op. ¶¶ 30–32. Unlike the majority, I would not be so quick to conclude that the federal third-party doctrine dictates a different result under the Fourth Amendment. As noted, the third-party doctrine cases cited by the majority ask whether individuals have a reasonable expectation of privacy in IP address data *itself*—not *other data* to which those IP addresses are directly linked. At stake here is Google search history information, which is as revealing as (if not more so than) the location data that *Carpenter* held lies beyond the reach of the third-party doctrine. *See Carpenter*, 138 S. Ct. at 2219–20 (declining to extend third-party doctrine to cell site location information given the privacy concerns implicated by the "revealing nature" of such information).

constitutional privacy interests at stake. *See People v. Tafoya*, 2021 CO 62, ¶ 47, 494 P.3d 613, 623 (explaining that intrusive, "cheap and surreptitious" surveillance techniques demand Fourth Amendment scrutiny because they "evade[] the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility'" (quoting *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring))). Indeed, courts must respond to the growing technological capabilities of law enforcement by continuing to apply the same "longstanding Fourth Amendment constitutional protections of individual privacy rights." *In re Search of: Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 756–57. The majority acknowledges this principle in theory, Maj. op. ¶ 24, but it is reluctant to apply it here. We should not hesitate where the conclusion is clear: the warrant here utterly lacked probable cause.

B. Particularity

¶112 Both the United States and Colorado constitutions explicitly require a warrant to describe with particularity *both* "the place to be searched" and "the things to be seized." *People v. Pacheco*, 175 P.3d 91, 94 (Colo. 2006).[6] These

[6] Despite certain differences in the text of article II, section 7 of the Colorado Constitution, our caselaw has consistently treated the particularity requirements of this provision synonymously with the Fourth Amendment. *E.g.*, *People v. Randolph*, 4 P.3d 477, 481 (Colo. 2000) (citing both the federal and Colorado constitutions for the proposition that "an affidavit must specify with particularity the places to be searched"); *People v. Ragulsky*, 518 P.2d 286, 287 & n.1 (Colo. 1974)

particularity requirements are critical because they "limit[] the authorization to search to the specific areas and things *for which there is probable cause to search*." *Garrison*, 480 U.S. at 84 (emphasis added). Where, as here, there is no probable cause with respect to the place to be searched, the warrant can neither "carefully tailor[] [the search] to its justifications" nor prevent the search from resembling "the wide-ranging exploratory searches the Framers intended to prohibit." *Id.*

¶113 The majority sidesteps this dual requirement by relying on the search terms to define both the place to be searched and the things to be seized. In the majority's view, the warrant was sufficiently particularized as to the *place* to be searched because the "narrow" search parameters (i.e., the nature of the keywords and the two-week timeframe) "dramatically reduce[d] the intrusiveness of the search." Maj. op. ¶¶ 45, 48. The majority further reasons that a "lightning-fast, digital," and "very cursor[y]" government examination of "unrelated documents" is too brief to "turn an adequately particularized search warrant into an unconstitutional general warrant." *Id.* at ¶ 47. But this approach erroneously conflates two distinct particularity requirements and allows technology to overtake the Constitution.

¶114 The majority's fundamental error lies in conflating the *place to be searched* with the *things to be seized*. The search parameters described the things to be seized:

(describing particularity with respect to the place to be searched as a "constitutional requirement" of both the federal and Colorado constitutions).

IP addresses linked to specific keyword searches conducted during a specific two-week period. But the fact that law enforcement is looking for something specific does not allow officers to look anywhere they want. The Fourth Amendment does not, to borrow a metaphor, permit law enforcement to probe every haystack on the planet simply because it is searching for a specific type of needle.

¶115 The majority's blessing of the particular search parameters used here gives one pause. True, an address might reflect the location of a private residence. But an address might instead reveal a person's search for the location of an abortion clinic, a church, a gun shop, a gay bar, a therapist's office, or a meeting place for Alcoholics Anonymous—any of which could be locations where a crime has taken place. But if any address corresponding to the location of a crime is sufficiently "narrow" to meet constitutional muster, one can imagine any number of keywords that would satisfy this standard. What about a search for the IP addresses of all Google users who searched for "mifepristone" or "gender-affirming care" or "Proud Boys" or "AR-15?" Each of these search queries could be potential evidence of criminal activity under some states' laws, depending on the circumstances. A two-week window does not necessarily solve the problem, either. Google receives *billions* of queries each *day*. Elec. Frontier Found. Brief, at 8–9. Given the "privacies of life" an address may reveal, Maj. op. ¶ 26 (quoting *Carpenter*, 138 S. Ct. at 2217), and the dubious degree to which a two-week

timeframe actually limits a search of Google's vast database, I cannot agree with the majority that the search parameters here necessarily reduced the intrusiveness of the search—"dramatically" or otherwise. *Id.* at ¶ 45. As noted, even here, the "narrow" search terms swept up the account information of two individuals that officers quickly eliminated as suspects and three others located outside of Colorado. *Id.* at ¶ 12.

¶116 That the search terms here yielded a limited number of results does not salvage the warrant. As a practical matter, law enforcement will never know how many results a reverse-keyword search will generate until *after* running the search. But "courts may not use the benefit of hindsight in evaluating application of the Fourth Amendment." *People v. Sotelo*, 2014 CO 74, ¶ 41, 336 P.3d 188, 196. And as stated above, our decision in *Gutierrez* instructs that, if anything, a miniscule number of "hits" produced by a global search only highlights the total "absence of any nexus" to "any evidence of wrongdoing" in the overwhelming percentage of accounts searched. 222 P.3d at 943–44.

¶117 Equally problematic is the majority's notion that because a computer (instead of human eyes) can search a billion Google user accounts with lightning speed, the government-directed computer search is no broader than the data it yields. Maj. op. ¶ 47. But for reasons I have already discussed, the fact that law enforcement places a digital filter between its officers' eyes and the full breadth of

accounts it has scanned neither reduces the intrusiveness of the search nor narrows the place to be searched.[7] Rather, the digital filter is the technological enhancement that *enables* the search to be so broad in the first place.

¶118 In any event, the fact that technology makes law enforcement's work faster and easier does not mean that its use avoids constitutional scrutiny—quite the opposite. Law enforcement may not wield "sense-enhancing technology," like the computer employed here, to obtain "information . . . that could not otherwise have been obtained without physical intrusion into a constitutionally protected area." *Kyllo*, 533 U.S. at 34. And even if law enforcement's use of such technology renders a search relatively non-invasive, the search remains subject to traditional Fourth Amendment constraints. *McKnight*, ¶ 54, 446 P.3d at 412.

¶119 The majority recognizes this principle, Maj. op. ¶ 24, but again fails to apply it. Instead, by sanctioning the practice here, the majority "leave[s] citizens 'at the

---

[7] Filters of this sort are, of course, required to place appropriate limits on the *items to be seized*, as our cell phone cases confirm. *E.g.*, *People v. Thompson*, 2021 CO 15, ¶ 19, 500 P.3d 1075, 1079 ("[A] warrant broadly authorizing police to search a cell phone *for* all texts, videos, pictures, contact lists, phone records, and any data showing ownership or possession violates the particularity demanded by the Fourth Amendment." (emphasis added)); *accord People v. Coke*, 2020 CO 28, ¶¶ 37–38, 461 P.3d 508, 516; *People v. Herrera*, 2015 CO 60, ¶¶ 19–20, 357 P.3d 1227, 1230–31. But contrary to the majority's suggestion, these cases do not address the lack of particularity with respect to the *place to be searched* at all, since these cases involve the search of a specific cell phone—that belonging to a *known suspect*. *E.g.*, *Thompson*, ¶¶ 4–5, 500 P.3d at 1077; *Coke*, ¶¶ 4–5, 461 P.3d at 511; *Herrera*, ¶ 2, 357 P.3d at 1228.

mercy of advancing technology'"—precisely what the majority purportedly seeks to avoid. *Id.* (quoting *Carpenter*, 138 S. Ct. at 2214).

VII. The Good-Faith Exception Does Not Apply

¶120 The majority ultimately concludes that the good-faith exception to the exclusionary rule renders moot any deficiencies in the warrant. In the majority's view, law enforcement "had no reason to know that it might have needed to demonstrate a connection between the alleged crime and Seymour's individual Google account" because, "until today, no court had established that individuals have a constitutionally protected privacy interest in their Google search history." *Id.* at ¶ 70. Because this view ignores the warrant's patent deficiencies—as well as the record—I cannot agree.

¶121 An officer's reliance on a warrant is unreasonable "where the warrant is so facially deficient that the officer cannot reasonably determine the particular place to be searched or things to be seized." *People v. Miller*, 75 P.3d 1108, 1114 (Colo. 2003). Here, the warrant does not identify the place to be searched at all—namely, a billion Google user accounts. This facial deficiency should alone suffice to conclude that the good-faith exception does not apply.

¶122 An officer's reliance on a warrant is also unreasonable when the "warrant [is] issued on the basis of a 'bare-bones' affidavit." *Gutierrez*, 222 P.3d at 941. "An affidavit that provides the details of an investigation, yet fails to establish a

minimal nexus between the criminal activity described and the place to be searched, is nevertheless bare-bones." *Id.* In *Gutierrez*, the supporting affidavit "fail[ed] to establish any connection at all between Gutierrez and criminal activity." *Id.* at 943. We therefore concluded that law enforcement's reliance upon it was unreasonable. *Id.* at 944.

¶123 Here, the affidavit detailed law enforcement's investigation efforts leading up to its request for the warrant. But as in *Gutierrez*, the affidavit provided no basis to believe that potentially incriminating evidence related to the arson was contained in the search histories held in Google's database of a billion user accounts (i.e., the place to be searched)—let alone in Seymour's specific user account. The lead investigator admitted as much during the suppression hearing. To the extent the majority concludes otherwise, it contradicts its own characterization of the affidavit as based on a "core premise" that is "at least debatable." Maj. op. ¶ 61.

¶124 Like this court in *Gutierrez*, I find it "difficult to understand how reasonably well-trained officers" searching through a billion individual Google user accounts, all but a handful 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." 222 P.3d at 944. For these reasons, I conclude that the good-faith exception is inapplicable here.

VIII. Conclusion

¶125 Longstanding Fourth Amendment principles still apply to law enforcement's use of advancing technology. *In re Search of: Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 756–57. Where law enforcement has probable cause to believe that a particular suspect's electronic device or digital account contains incriminating evidence, officers routinely obtain a warrant, consistent with the Fourth Amendment, to search that device or account for particular evidence. But that is not what happened here.

¶126 Here, law enforcement's diligent investigative efforts proved fruitless. And so, out of leads, law enforcement obtained a warrant to search a billion Google users' data to generate a list of possible suspects—based not on probable cause, but solely on law enforcement's hunch that the perpetrator may have searched the address where the arson took place.

¶127 There is certainly temptation here to reward creative police work, particularly when it results in the apprehension of the suspected perpetrators of a senseless arson and murder of five individuals. When a protracted investigation produced no results, an investigator's clever hunch, combined with cheap and convenient technology, led to an important break in the case. However, "[n]owhere in Fourth Amendment jurisprudence has the end been held to justify

unconstitutional means." *Id.* at 757. The guiding principle simply cannot be that when leads dry up and all else fails, we break the Constitution.

¶128 Nothing about the majority's opinion restricts reverse-keyword searches to a tool of last resort. Police departments across the country are already employing similar warrants as a matter of routine, even when they have other leads. Love & Alba, *supra*. Indeed, Google received 60,472 search warrants in the United States in 2022, and it provided information in 80% of those cases. *Id.*

¶129 At the risk of sounding alarmist, I fear that by upholding this practice, the majority's ruling today gives constitutional cover to law enforcement seeking unprecedented access to the private lives of individuals not just in Colorado, but across the globe. And I fear that today's decision invites courts nationwide to do the same.

¶130 I respectfully dissent.