DATE FILED: March 7, 2023 5:08 PM
FILING ID: 2BBB22A1761D6
CASE NUMBER: 2023SA12

Colorado Supreme Court
2 East 14th Avenue
Denver, CO 80203

Original Proceeding
District Court, City and County of Denver
Hon. Martin Egelhoff
Case No. 21CR20001

IN RE

THE PEOPLE OF THE STATE OF COLORADO,

Plaintiff-Respondent,

v.

GAVIN SEYMOUR,

Defendant-Petitioner.

▲ COURT USE ONLY ▲

Case Number: 23SA12

Katherine A. Hansen, Reg. No. 25464
Senior Deputy District Attorney
Joseph M. Morales, Reg. No. 24706
Chief Deputy District Attorney
Courtney L. Johnston, Reg. No. 39266
Chief Deputy District Attorney

Beth McCann, Denver District Attorney
201 West Colfax Ave., Dept. 801
Denver, CO 80202
720.913.9000

Katherine.Hansen@DenverDA.org

People's Response to Gavin Seymour's C.A.R. 21 Petition

CERTIFICATE OF COMPLIANCE

I certify that this response does not comply with all applicable requirements of C.A.R. 28(g) and C.A.R. 32. *See* C.A.R. 21(i).

- The response contains 10,547 words. It therefore does not comply with the word limit set forth in C.A.R. 28(g). A motion to exceed the word limit will be filed in conjunction with the filing of this brief.
- The response complies with the formatting requirements set forth in C.A.R. 32(a).

I acknowledge that this response may be stricken if it fails to comply with the governing rules.

s/ Katherine A. Hansen
Katherine A. Hansen
Senior Deputy District Attorney

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Constitutional Provisions

INTRODUCTION

Gavin Seymour challenges the district court's order denying his motion to suppress evidence obtained from a Google keyword search warrant. Because the district court properly ruled that the warrant satisfied constitutional requirements, the rule to show cause should be discharged.

STATEMENT OF THE CASE AND FACTS

The crime and investigation. In the early morning of August 5, 2020, Denver Police Officers and Denver Firefighters were dispatched to a house fire at 5312 N. Truckee Street in Denver (Pet. Exhibit 9, pp15-16). The house was fully engulfed in fire (Pet. Exhibit 9, p16). Five individuals – Khadija Diol (1 year old), Hawa Beye (7 months old), Adja Diol, (23 years old), Djibril Diol (29 years old), and Hassan Diol (25 years old) – were pronounced dead on the scene (Pet. Exhibit 9, pp23-24,37). Three occupants had escaped through a second story window and sustained injuries from the fall (Pet. Exhibit 9, pp20,26).

Surveillance footage from neighbors' cameras showed three masked individuals standing in the side yard of the victims' home before the fire began (Pet. Exhibit 9, pp28-29). The individuals were wearing dark hooded sweatshirts and dark masks (Pet. Exhibit 9, pp29-30). At one point, these individuals were pointing to an area on the northeast corner of the victim's home (Pet. Exhibit 9, p31). Soon thereafter, these

individuals were seen running westbound from the backyard area of the victims' home through the side yard and out the gate towards the front of the residence (Pet. Exhibit 9, p32). Within seconds, a camera located on the northeast corner of the neighbor's residence captured flames coming out of the lower level of the home (Pet. Exhibit 9, pp32-33).

Arson investigators determined that an accelerant was used to start the fire, which began in the rear of the residence where the suspects were observed (Pet. Exhibit 9, p34). Signs of an accelerant were found inside the home as well as outside the residence near where the suspect vehicle had been parked (Pet. Exhibit 9, pp34-35).

After a lengthy investigation, detectives were unable to identify the suspects or determine a motive for the arson, although they believed it was a targeted attack (Pet. Exhibit 9, p46). The residence at 5312 N. Truckee Street is single family home in a densely populated subdivision and is not a house that would likely be picked at random (Pet. Exhibit 9, p17,46-47). It was not on a corner lot, but instead located between numerous other residences (Pet. Exhibit 9, pp17,46-47). The suspects had been dressed to conceal their identity and brought the gas can with them, indicating that the offense was pre-planned (Pet. Exhibit 9, p46).

The Google keyword warrant. Multiple warrants were obtained in an attempt to identify the suspects, but these strategies proved unsuccessful (Pet. Exhibit 9, pp28,46). Therefore, police pursued a new approach – seeking to identifying anyone who may have searched for the victims' address prior to the offense (Pet. Exhibit 9, pp48,131).

Detectives ultimately submitted three warrants to Google for this information. The first two were withdrawn because the language used in the warrant did not comply with Google's internal requirements (Pet. Exhibit 4, p6).

A third warrant was obtained and submitted to Google (Pet. Exhibit 4, pp6-7; Pet. Exhibit 9, p48-49).[1] The records that were then produced by Google included a spreadsheet of IP addresses associated with the responsive searches of the victims' address (including all variations of the address) that occurred in the approximately two weeks prior to the offense, along with a list of de-identified users that conducted these searches (Pet. Exhibit 4, p7; Pet. Exhibit 9, pp132-136,196). The query had returned 61 responsive searches.

[1] Although one of the detectives testified at the preliminary hearing that he "believed" that warrant had been limited to searches conducted in Colorado, he was mistaken (Pet. Exhibit 9, p82). Notably, he was not the affiant of the Google keyword search warrant.

Although five anonymous Google "accounts" had been associated with qualifying searches, in order to identify the subscriber or physical locations of those users, additional search warrants had to be submitted to the Internet Service Provider ("ISP") or wireless carrier that provided the IP address for the search. These warrants would request that the ISP or wireless carrier identify the person or location assigned to that particular IP address. Through that process, detectives would then be able to identify the individuals who had conducted the searches (Pet. Exhibit 9, pp49,135-136,193).

Further investigation. Warrants were obtained to identify the actual the source of the IP addresses.[2] Through those efforts, four suspects were identified: Tanya Bui, Kevin Bui, D.S. and Gavin Seymour (Pet. Exhibit 9, pp49,52).

A subsequent investigation, including additional digital evidence warrants and traditional investigative strategies, revealed substantial proof that Kevin Bui, Seymour, and D.S. had committed the arson/homicide (Pet. Exhibit 9, pp50-57,86-87,139-147). All three suspects were arrested (Pet. Exhibit 9, p57). Kevin Bui acknowledged their involvement in these crimes (Pet. Exhibit 9, pp57-59). He explained that he was

[2] One account was associated with Mami Diol, a family member of the victims, and one was associated with another individual who was eventually excluded because she had no apparent connection to the crime or to the three suspects (Pet. Exhibit 9, pp138-139).

robbed in July while attempting to purchase a gun and his phone was stolen; he tracked the phone using the "Find My iPhone" app and it "pinged" back to 5312 Truckee Street (Pet. Exhibit 9, p59).

Gavin Seymour was charged with multiple felonies, including five counts of first-degree murder. He has pled not guilty.

District court proceedings. Seymour filed motions to suppress various search warrants that were issued during the investigative stage of this case. At issue here is the Google keyword warrant (Pet. Exhibit 16).

At the suppression hearing, a representative from Google testified about the process used to respond to the keyword warrant (Pet. Exhibit 10). She first explained that an authenticated user is someone who is signed into their Google account ("GAIA ID"), and an unauthenticated user is someone who uses Google but is not signed into an account (Pet. Exhibit 10, pp27-28). Authenticated users have the ability to delete their searches (Pet. Exhibit 10, p29). If an unauthenticated user conducts a search, that search is identified by a browser cookie ID (Pet. Exhibit 10, p30).

When Google receives a keyword search warrant, it conducts a query of its database using the search parameters in the warrant (Pet. Exhibit 10, pp33-34,36-38). This search cannot be limited to any particular geographic area (Pet. Exhibit 10, pp40-

41). The results are anonymized so that the sources of the searches (both GAIA IDs and browser cookie IDs) are not discernable without further legal process (Pet. Exhibit 10, pp47,50).

In this case, the query returned 61 responsive searches that were associated with 5 unique GAIA IDs and 3 unique browser cookie IDs (Pet. Exhibit 4, p7).

Detective Ernest Sandoval, the affiant of the keyword search warrant, also testified at this hearing (Pet. Exhibit 10, p68). He acknowledged that he had never used a keyword search warrant before, nor did the Denver Police Department have policies and procedures for keyword search warrants (Pet. Exhibit 10, pp69-70). He acknowledged having submitted two keyword search warrants that Google did not execute because they did not comply with Google's internal policies (Pet. Exhibit 10, pp71,76). After consultation with Google and the DA's office, a third keyword warrant was drafted and submitted (Pet. Exhibit 10, p77). This third warrant did not mention the previous two (Pet. Exhibit 10, p77).

When asked if he ever told the judge that a keyword warrant would require Google to search "billions of people," Detective Sandoval indicated that he did not know what Google did to conduct this search (Pet. Exhibit 10, pp78-79). He stated that the police were only interested in searches that had been conducted in Colorado

(Pet. Exhibit 10, p80).[3] Once the police received the data from Google, they planned to conduct an open-source inquiry to determine which IP addresses originated in Colorado. They would then submit another search warrant to identify the location and subscriber associated with the IP address (Pet. Exhibit 10, pp87-88).

Following the hearing, the parties submitted written arguments on all of the motions to suppress, including the Google keyword search warrant (Pet. Exhibits 5, 6, 7; People's Exhibit A).

After being fully advised, the district court issued an oral ruling denying the motions to suppress (Pet. Exhibit 8). With regard to the Google keyword search warrant, the court noted that Seymour did not have standing to assert a violation of privacy as to the accounts of others (Pet. Exhibit 8, p22). However, he did have a reasonable expectation of privacy in *his own* Google account data (Pet. Exhibit 8, p23).

The court noted that law enforcement did, however, obtain a warrant for this data (Pet. Exhibit 8, pp23-24). The court rejected the defense's arguments concerning the scope of the search (i.e., that it was a search of "billions of people"), finding that it

[3] Although Detective Sandoval agreed that the surveillance video obtained during the investigation did not establish whether the suspects had a cellphone, were using their cellphones, or were conducting a keyword search (Pet. Exhibit 10, pp81-82), this concession is irrelevant to the issues presented in this case because the warrant was seeking information about searches conducted for this address prior to the offense. *See* Pet. Exhibit 10, p115.

was "a database query…which established certain search parameters that were within the capacity of this database" (Pet. Exhibit 8, pp20,25). The court also characterized the search as involving "a very particular, specific targeted category of data" (Pet. Exhibit 8, p25).

The court found that there was probable cause to support the search warrant (Pet. Exhibit 8, pp26-28). The court noted that the affidavit included "very specific factual assertions with respect to why the police and why a magistrate would believe that there's a likelihood…that folks would use the internet to do that research and find those directions" (Pet. Exhibit 8, pp26-27). With regard to particularity, the court found that the warrant was "narrowly tailored" and "not overbroad" (Pet. Exhibit 8, pp27,28).

The court found no false statements or reckless misrepresentations in the warrant, first noting that the detective need not have advised the magistrate that it would involve a search of "billions" of people because "[t]hat's just not what the search warrant does" (Pet. Exhibit 8, p28). The court also ruled that it was not necessary to reference the two previous warrants because those details would not "impact the probable cause determination" (Pet. Exhibit 8, p29).

The court found that it was not "necessary" to invoke the good faith exception because the warrant was "completely valid" (Pet. Exhibit 8, p29). However, the court

also observed that this keyword search warrant was novel to law enforcement (Pet. Exhibit 8, p28). The court further ruled that, "given the specificity of this particular warrant and the magistrate's review," it would "defy common sense and comprehension…that somehow any of the criteria for the [exceptions to the] good faith exception would come into play that would not allow that exception to be applicable" (Pet. Exhibit 8, pp29-30). The court ruled that law enforcement reasonably relied on the warrant (Pet. Exhibit 8, p30).

The court ultimately denied the motion to suppress the Google keyword search warrant (Pet. Exhibit 8, pp35,40). The court concluded with the following observation:

> I just want to say, based upon my review of all this, it is my judgment that the police in this case did exactly what we want the police to do, i.e., be careful, be specific, be particular in terms of judicial process to obtain this information. Quite frankly, I think if the Court were to determine, based upon all of these things they did and the specificity which I found, if that somehow is beyond what the Fourth Amendment requires, that's -- I find that hard to understand and believe. I think the police here did exactly what we want them to do.

(Pet. Exhibit 8, pp44-45).

Seymour then filed a petition in this Court for relief pursuant to C.A.R. 21, challenging only the ruling as to the Google keyword search warrant.

SUMMARY OF THE ARGUMENT

The district court properly denied Seymour's motion to suppress the results of the Google keyword search warrant. Despite Seymour's claims to the contrary, the search warrant did not involve a search of a "billion" people or accounts. Even if it did, he does not have standing to challenge a search of any account other than his own.

The keyword at issue here was an *address for a private residence* – not the type of information associated with expressive activities, and therefore the First Amendment is not implicated.

The Google keyword warrant satisfied the constitutional requirements that 1) the place to be searched be stated with specificity, 2) the data to be received be identified with particularity, and 3) there was probable cause to believe that evidence of this crime – the heinous arson and homicide of five innocent people – would be found in the data being requested.

But, even if the warrant was somehow deficient, the Denver Police Department detectives reasonably relied on the warrant in good faith; therefore, suppression wouldn't be warranted.

ARGUMENT

The questions properly before this Court are 1) whether the Google keyword search warrant violates the Fourth Amendment of the United States Constitution and Article II, Section 7 of the Colorado Constitution and, if so, 2) whether the good faith exception applies.

A. Burden of Proof and Standard of Review.

When reviewing the sufficiency of a warrant affidavit, a judge's probable cause determination is given great deference and is not reviewed de novo. *People v. Pacheco*, 175 P.3d 91, 94 (Colo. 2006); *Henderson v. People*, 879 P.2d 383, 391 (Colo. 1994); *People v. Leftwich*, 869 P.2d 1260 (Colo. 1994); *People v. Titus*, 880 P.2d 148, 150 (Colo. 1994). "[A] reviewing court should presume the affidavit is valid…." *People v. McKay*, 513 P.3d 347, 349 (Colo. 2021). The duty of the court reviewing the sufficiency of the warrant affidavit is simply to ensure that the issuing judge had a substantial basis for concluding that probable cause existed. *People v. Pate*, 878 P.2d 685 (Colo. 1994); *People v. Wilson*, 819 P.2d 510, 513 (Colo. App. 1991); *Titus*, 880 P.2d at 150. In making that determination, the reviewing court must restrict itself to the four corners of the affidavit and must analyze the affidavit in a practical, nontechnical, and common-sense fashion. *People v. Atley*, 727 P.2d 376, 377 (Colo. 1986); *Wilson*, 819 P.2d at 513; *Titus*, 880 P.2d at 150. Seymour's invitations to consider the practical

impact and collateral consequences that this Court's ruling may have on other scenarios should be rejected.

B. Scope of the search.

When determining whether the keyword search was constitutional, it is important to understand the true nature of the search, including the method by which the requested information was obtained.

Seymour relies heavily on the assertion that the warrant required Google to search "billions" of Google users to locate those who conducted a qualifying search. These arguments ignore the very evidence he solicited from Google.

The search conducted by Google was not of "people" or "users," but of a database comprised of digital data. Google typed in search parameters (at its base level – numbers and letters) and directed its computer algorithms to identify matches between the numbers and letters input (at their base level, ones and zeroes) and the combinations of ones and zeroes already contained within its database (*See* Pet. Exhibit 4, p3).

Seymour would have this Court ignore the realities of what occurred in this case, and instead treat a database inquiry the same as if a Google employee opened a file for each account and conducted a visual review of all of the searches performed by that user to determine whether that user submitted a search with terms matching

those provided in the warrant, and then repeated that "search" a "billion" times over. To the contrary, here a database was accessed, and the only information actually observed was a list of accounts that had conducted a search that included one or more of the narrow search terms listed in the warrant (*See* Pet. Exhibit 4, pp3-4).

The database query was not a visual "search" of Google's database. No one ever saw the contents of users' searches that didn't satisfy the criteria in the warrant.[4] A "search" occurs where an expectation of privacy that society is prepared to consider reasonable is *infringed*. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). Where Google did not actually observe the nonresponsive data, it simply cannot be said that any privacy rights associated with the non-qualifying searches were infringed upon.

Indeed, data files in a computer are essentially combinations of ones and zeroes. *See* https://www.techopedia.com/definition/17929/binary-data ("Binary data is a type of data that is represented or displayed in the binary numeral system. Binary data is the only category of data that can be directly understood and executed by a computer. It is numerically represented by a combination of zeros and ones.");

[4] Consider again a scenario where a warrant is issued for a particular individual's bank records. The bank receives the warrant and conducts a computer query of its bank records database to retrieve the responsive information. In this scenario, the bank is not looking through every account of every customer. Moreover, to suggest that the warrant must have provided probable cause for each of the bank's customers in order to even comply with the warrant directed at one customer would be nonsensical.

https://en.wikipedia.org/wiki/Computer_data_storage (A modern digital computer represents data using the binary numeral system. Text, numbers, pictures, audio, and nearly any other form of information can be converted into a string of bits, or binary digits, each of which has a value of 0 or 1). The database itself was not read, observed, or visualized in a manner that would have allowed Google to see the contents of any of the searches that were conducted by Google users *other than* the ones that matched the keyword terms in the warrant.

The results provided to the police included an anonymized account or user identifier to associate a particular user (known to Google but unknown to law enforcement) to the address search (Pet. Exhibit 4, p4).[5] Pursuant to the warrant, Google was ordered to provide two types of information; 1) an anonymized list of users who conducted a search including the specified keywords during the time period of July 22, 2020 at 12:01 a.m., through and including August 5, 2020 at 2:45 a.m.; and 2) the full IP addresses of each qualifying search (Pet. Exhibit 16).

Seymour argues that the full IP addresses rendered "meaningless" the anonymization of the associated user because those IP addresses "are not anonymous

[5] Although Google recognized that some warrants may authorize law enforcement to request additional follow-up information without subsequent legal process (Pet. Exhibit 4, p4), such a practice is not at issue here because the initial keyword warrant issued in this case did not authorize any further information without additional legal process.

identifiers" and "[l]aw enforcement can easily associate an IP address with a particular subscriber or street address." That is misleading.

An IP address "is the unique address assigned to a particular [device] connected to the Internet." *People v. Garrison*, 411 P.3d 270, 275 (Colo. App. 2017). Although IP addresses can be linked to a device/router used to conduct the search, the identifying information for the IP source cannot be ascertained (and was not obtained in this case) without additional legal process. IP addresses can be searched through publicly available resources to identify their general source (ISP or wireless carrier), and sometimes their general location (a state or city). But information identifying the *actual* source (the subscriber of the device or the physical location of the router) is maintained by the ISP, and these companies (Comcast/Xfinity, T Mobile, etc.) require legal process before they will provide information linking a particular IP address to a person or location.[6] *See State v. Reid*, 945 A.2d 26, 28–29 (N.J. 2008) ("Only the ISP can match the name of the customer to a dynamic IP address."); *BMG Rts. Mgmt. (US) LLC v. Cox Commc'ns, Inc.*, 881 F.3d 293, 299 (4th Cir. 2018) (recognizing as a factual matter "only the ISP can match the IP address to the subscriber's identity").

[6] Although in some jurisdictions a subpoena may be used to obtain this information, Colorado law does not grant subpoena power to law enforcement during the investigative stage of a case and therefore a warrant was required by the carriers/ISPs and was, in fact, obtained in this case. *See, e.g.*, § 16-3-301, C.R.S. (2022); Crim. P. 41.

Moreover, if the police want a search warrant requiring an ISP to identify the subscriber or physical location of an IP address, then they have to show probable cause establishing a nexus between that IP address and evidence of criminal activity. This process was completed in this case.

Seymour further complains that because Google included additional search terms beyond the specified terms listed in the warrant, this undermined the validity of the warrant. But here, the warrant did not specifically limit the production to only those accounts that used a listed keyword term standing alone. The warrant asked Google to identify the accounts that "conducted a search while using Google Services … ***using*** any one or more of the following the search terms…" (Pet. Exhibit 16) (emphasis added). Searches that included a keyword term alone would qualify, as would searches that included a keyword term alongside others, such as "5312 N. Truckee Street Denver" or "5312 N. Truckee Street Denver, Colorado." Both examples "used" a keyword term and would therefore be subject to inclusion. And, as the Google custodian noted, Google's general practice is to include all responses that contain the identified word or phrase, even if the search also included additional words (Pet. Exhibit 4, pp3-4).

Seymour also argues that including additional terms constituted an "overbroad *execution*" of the warrant. However, even if the execution were overbroad (which it

wasn't), Seymour fails to cite to any legal authority suggesting that a warrant can be invalidated when materials outside the scope of the warrant are provided by a third party.

Indeed, the purpose of the exclusionary rule is to deter police misconduct, and the rule should not be applied in circumstances where this purpose will not be served. *Casillas v. People*, 427 P.3d 804, 810 (Colo. 2018) (citing *Davis v. United States*, 564 U.S. 229, 237 (2011) and *Herring v. United States*, 555 U.S. 135, 144 (2009)) ("To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system."). It cannot be said that suppressing evidence obtained from a valid warrant simply because a third party provided materials outside the scope of that warrant (something wholly outside of law enforcement's control) would deter future police misconduct.

Finally, Seymour argues that the search in this case implicated the First Amendment, suggesting that all keyword searches have the "potential" to burden an individual's freedom of inquiry and association.

In considering this argument, it is important to remember that, when conducting the query of its database, Google is not actually viewing any search history, other than the responsive results of the query. Therefore, if the search is for

words or phrases that do not implicate expressive activity, as this search was, no information about the searches conducted by others is actually viewed.

Moreover, in most circumstances, a search for an address is not a search that would implicate the type of "expressive activities" or "free exchange of ideas" that require the balancing analysis set forth in *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1051 (Colo. 2002), which held that the First Amendment and Article II, Section 10 of the Colorado Constitution "safeguard the right of the public to buy and read books anonymously, free from governmental intrusion." While there may be some factual scenarios where a search for a street address implicates the First Amendment, the search for "5312 N. Truckee Street" is not one of them.

Moreover, even if the First Amendment were implicated here, the keyword search warrant would unquestionably survive the scrutiny dictated by *Tattered Cover*: 1) there was a compelling need for this information, as the suspects in this horrific crime had evaded detection for months; 2) there was a direct nexus between the matter being investigated (an arson/homicide committed at a particular targeted residence) and the material sought (users who conducted a search for this address); 3) all other investigative strategies had failed to yield fruitful leads and there did not appear to be other reasonable methods of identifying the suspects; and 4) the scope of the search was extremely narrow – an anonymized list of users who conducted the search in a

short period before the offense – and did not seek out persons who had searched for the type of "expressive ideas" that would raise First Amendment concerns.

Neither this Court nor the United States Supreme Court have ever precluded an entire law enforcement investigative strategy based on the possibility that, in some circumstances, it might be abused or otherwise infringe on other constitutional rights. To do so would be akin to legislative action, and "courts must avoid making decisions that are intrinsically legislative. It is not up to the court to make policy or to weigh policy." *Town of Telluride v. Lot Thirty-Four Venture, L.L.C.*, 3 P.3d 30, 38 (Colo. 2000). Whether or not keyword search warrants should be wholly banned because they *may* infringe on the right to search for highly personal matters is a matter to be left to the legislature. *See, e.g.*, *United States v. Chatrie*, 590 F. Supp. 3d 901, 926 (E.D. Va. 2022) (noting that questions relating to the permissibility of certain investigative techniques involving technology are "matters … best left to legislatures"). Cases interpreting the Fourth Amendment have always avoided bright line rules, *Ohio v. Robinette*, 519 U.S. 33, 39 (1996) ("the touchstone of the Fourth Amendment is reasonableness," not "bright-line rules"), and prohibiting an entire search mechanism because it may run

afoul of some other law or constitutional provision under certain circumstances would be simply unprecedented.[7]

> [W]ith any warrant request, the Fourth Amendment principles of probable cause and particularity will guide the analysis rather than proclamations about whether requests for evidence impacted by new technology are *per se* unconstitutional. The Supreme Court, when considering the impact of new technology, has done exactly that in deciding whether a warrant is necessary to obtain data stemming from new technology.

Matter of Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345, 363 (N.D. Ill. 2020).

C. Expectation of Privacy and Standing

The burden of establishing a protected Fourth Amendment privacy interest rests squarely with an individual defendant. *Rawlings v. Kentucky*, 448 U.S. 98, 104 (1980); *see also People v. Curtis*, 959 P.2d 434, 437 (Colo. 1998). "Fourth Amendment rights are personal [and] ... may not be vicariously asserted." *Alderman v. United States*, 394 U.S. 165, 174 (1969); *see also People v. Galvadon*, 103 P.3d 923 (Colo. 2005) ("suppression of the product of a violation of the Fourth Amendment's prohibition

[7] Consider, for example, a scenario where an unknown suspect tells his victim, during a crime, that he found the victim by conducting a Google search for his address, then proceeds to assault the victim or damage his home. It would unquestionably be appropriate to submit a warrant to see who had searched for the victim's address in this scenario. A bright line rule prohibiting keyword searches, however, would preclude this clearly appropriate inquiry.

against unreasonable searches and seizures can be successfully urged only by those whose rights were violated by the search itself").

Seymour's arguments rely heavily on the notion that the search in this case constituted a search of "billions" of users. As demonstrated above, that proposition is incorrect. Moreover, Seymour has no standing to object to a search of any account other than his own. *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978); *Alderman*, 394 U.S. at 183; *People v. Juarez*, 770 P.2d 1286, 1288 (Colo. 1989). This Court should focus only on Seymour's search for the victims' address.

Because a warrant was in fact obtained in this case, it is unnecessary to decide the "murky" question of whether an individual has a legitimate expectation of privacy in the searches they conduct on a third-party application or website. *See Matter of Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d at 360 (court declined to reach standing issue "because the government has chosen to obtain a warrant to obtain the geofence data based on a showing of probable cause"); *Byrd v. United States*, 138 S. Ct. 1518, 1530 (2018) (Fourth Amendment standing it is not a jurisdictional question and need not be addressed before addressing the merits of a Fourth Amendment claim); *United States v. Rhine*, 2023 WL 372044, at *27 (D.D.C. Jan. 24, 2023) (following the path taken by numerous other jurisdictions addressing Google geofence warrants in declining to

reach the issue of Fourth Amendment standing). This clearly complicated issue is best left to a case that requires its resolution.

D. The Keyword Warrant was Constitutional

For a warrant to be constitutionally valid, it must satisfy three general requirements: 1) particularity in the location to be searched; 2) particularity in the items to be seized; and 3) probable cause to believe that the items to be seized are in the location to be searched. U.S. Const. amend IV; Colo. Const. art. II, § 7; *Groh v. Ramirez*, 540 U.S. 551, 557 (2004); *People v. Cox*, 429 P.3d 75, 78 (Colo. 2018).

Ultimately, the touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined by assessing the degree to which it intrudes upon an individual's privacy and the degree to which it is needed to promote legitimate governmental interests. *United States v. Knights*, 534 U.S. 112, 118-19 (2001).

1. Particularity in the location to be searched.

"The test for determining the adequacy of the description of the location to be searched is whether the description is sufficient to enable the executing officer to locate and identify the premises with reasonable effort, and whether there is any reasonable probability that another premise might be mistakenly searched." *Harman v. Pollock*, 446 F.3d 1069, 1078 (10th Cir. 2006). Where, as here, the items being searched are records maintained by a third-party business entity, it is instructive to

consider the language of §16-3-301.1, which addresses court orders for the production of records.

Under § 16-3-301.1(3)(a)(I), the affidavit must identify or describe "the business entity that is in actual or constructive control of the records." By listing Google as the entity in control of the records being sought, and providing its address and registered agent, the location to be searched was adequately described.

Seymour does not dispute that the records being sought were in the custody and control of Google. Rather, he contends that, instead of simply identifying Google and its address as the location to be searched, the warrant also had to identify each specific account contained in the database to be searched. This argument strains credulity and is not supported by any legal authority.

2. Particularity in the data to be searched and seized.

So-called "general warrants," which permit "a general, exploratory rummaging in a person's belongings," are prohibited. *People v. Coke*, 461 P.3d 508, 516 (Colo. 2020); *People v. Herrera*, 357 P.3d 1227 (Colo. 2015). To prevent general, exploratory searches, the Fourth Amendment requires a particular description of the things to be seized. *People v. Noble*, 635 P.2d 203, 209 (Colo. 1981) ("[T]he description [in the warrant] of the property to be seized should be such that 'the officer charged with the

duty of executing the warrant will be advised with a reasonable degree of certainty of the property to be seized.'" (Citations omitted)).

In other words, "[t]he requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is taken, nothing is left to the discretion of the officer executing the warrant." *People v. Roccaforte*, 919 P.3d 799, 802 (Colo. 1996).

In the context of business records, the warrant must "identify or describe, as nearly as may be, the records that shall be produced." § 16-3-301.1(3)(a)(II). Considered in conjunction with the Fourth Amendment particularity requirement, this requirement is met if the warrant describes the data to be seized with sufficient detail to allow the person conducting the search (in this case, Google) to know what data is encompassed within the warrant's authorization (i.e., which data they are authorized to release to the requestor). When this occurs, the warrant is not a "general warrant," and this constitutional requirement is met.

Here, the keyword search warrant asked Google to locate and provide two pieces of information: 1) users (de-identified) that had conducted a search of a particular residential address (using several variations of that address) during a specified, narrow time period, and 2) the IP addresses associated with each responsive

search. These parameters clearly indicated to the entity in possession of the records what they were authorized to provide to the requestor.

A warrant is not constitutionally "overbroad" simply because it authorizes a search and seizure of a potentially large amount of data. A warrant is "overbroad" when the probable cause in the affidavit is insufficient to justify a search of one or more of the items listed as "items to be seized." See *Roccaforte*, 919 P.2d at 802 ("The primary function of the particularity requirement of the Warrants Clause is to ensure that government searches are 'confined in scope to particularly described evidence relating to a specific crime for which there is demonstrated probable cause.'" (citing *Voss v. Bergsgaard*, 774 F.2d 402, 404 (10th Cir. 1985))); *see also United States v Kidd*, 386 F. Supp. 3d 364 (S.D.N.Y. 2019) (a warrant is overbroad if its description of the objects to be seized is broader than can be justified by the probable cause upon which the warrant is based); *United States v Wey*, 256 F Supp 3d 355 (S.D.N.Y 2017) (a search warrant is legally invalid for overbreadth to the extent it permits officers to search or seize items without probable cause that they contain evidence of a crime); *Matter of Search of Info. that is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d 62, 76 (D.D.C. 2021) ("A warrant is not constitutionally overbroad so long as the time, location, and overall scope of the search are consistent with the probable cause set

forth in the warrant application."). As demonstrated below, there was ample probable cause to support this warrant.

The test for particularity "is a pragmatic one" that "may necessarily vary according to the circumstances and type of items involved." *United States v. Torch*, 609 F.2d 1088, 1090 (4th Cir. 1979) (quoting *United States v. Davis*, 542 F.2d 743, 745 (8th Cir. 1976)). Here, the circumstances involved a query search of a computer database, not a visual search of data, using very narrow parameters: a specific address searched within a 2-week period. *Matter of Search of Info. that is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d at 75 ("[S]earch warrants must be specific.").

In this circumstance, the warrant was required to identify the specific data to be searched for and provided. The warrant satisfied this requirement.

3. Probable cause to believe that evidence relevant to the arson/homicide would be located in the data requested.

Probable cause for a search exists when the affidavit in support of the warrant alleges sufficient facts to cause a person of reasonable caution to believe that contraband or other evidence of criminal activity is located at the place to be searched. *E.g.*, *Henderson*, 879 P.2d at 391.

The following principles provide important guideposts for all probable cause analysis:

- The task of the issuing magistrate is simply to make a practical, common-sense decision whether given all the circumstances set forth in the affidavit before him there is a *fair probability* that contraband or evidence of a crime will be found in a particular place.
- Probable cause determinations must be approached in a practical way because probable cause is a flexible common-sense standard.
- Probable cause is a fluid concept, turning on the assessment of probabilities in particular factual contexts, not readily, or even usefully, reduced to a neat set of legal rules.
- Probable cause is more than a mere suspicion, but considerably less than what is necessary to convict someone.
- Probable cause does not deal with hard certainties, but with probabilities.
- The court must look at the totality of the circumstances as set forth in the affidavit to determine whether probable cause exists.
- Such a determination requires courts to consider the cumulative weight of the information in connection with reasonable inferences that the officer is permitted to make based upon the officer's specialized training and experiences.

- The probable cause standard does not demand any showing that a good-faith belief be correct or more likely true than false; rather, it requires only such facts as make wrongdoing or the discovery of evidence thereof probable.
- A probable cause determination does not require absolute certainty that evidence of criminal activity will be found at a particular place.
- A search warrant application is not required to guarantee that evidence will be found.
- Finely tuned standards such as proof beyond a reasonable doubt or by a preponderance of the evidence, useful in formal trials, have no place in the probable-cause decision.
- Probable cause may be based on common-sense conclusions about human behavior.
- The preference for warrants is most appropriately effectuated by according great deference to a magistrate's determination.
- Probable cause is not a high bar.

See, e.g., *Kaley v. United States,* 571 U.S. 320, 338-39 (2014); *Illinois v. Gates*, 462 U.S. 213, 238 (1983); *Texas v. Brown*, 460 U.S. 730, 742 (1983); *Maryland v. Pringle*, 540 U.S. 366, 370 (2003); *United States v. Arvizu*, 534 U.S. 266, 27 (2002); *People v. Crippen*, 223 P.3d 114, 117 (Colo. 2010).

Probable cause does not depend on *direct evidence* or *personal knowledge* that evidence is located in the place to be searched; "it is enough when the affidavit establishes a nexus between the objects to be seized and the place to be searched from which a person of reasonable caution would believe that the articles sought would be found there." *United States v. Hargus*, 128 F.3d 1358, 1362 (10th Cir. 1997); *Ornelas v. United States*, 517 U.S. 690, 700 (1996) (a warrant affidavit need not include direct evidence that the evidence sought would be found in the place to be searched – "direct evidence has never been required by the Fourth Amendment"). Here, the detectives were not required to establish that the suspects did, in fact, conduct a search for the victims' address. They were simply required to establish that it was reasonable to believe that they did.

In this affidavit, the historical facts and reasonable inferences therefrom created a "fair probability" that evidence related to this arson/homicide would be found in the requested Google data, i.e., persons who searched for the victims' address in the approximately two weeks prior to the offense. In addition to the facts set forth regarding the crime itself and information learned in the ensuing investigation, the affidavit specifically explained why it was reasonable to believe that the persons involved in this crime (known to be at least three suspects) would have searched the address where the fire occurred prior to the offense:

> Based on the extreme nature of this crime and the extensive planning it must have taken to carry out the events involved in this offense, Your Affiant feels that this crime was very personal and involved a substantial amount of anger towards someone in the victim residence and/or was intended to send some sort of message. This belief is based on years of investigation of violent crimes and the motives associated with such crimes that Your Affiant has been exposed to over the years. Considering the personal nature of this offense, the actions of the suspects as observed on the surveillance videos, and the amount of planning that likely went into a coordinated attack such as this one, Your Affiant believes that there is a reasonable probability that one or more of the suspects searched for directions to the victim's address prior to the fire.
>
> The victim's home is in a densely populated subdivision and does not "stick out" as a house that would likely have been picked at random. It is not on a corner lot, which would be an easier target residence as there would be more area to move in before and after setting the fire. As such, it is reasonable to believe that this home was targeted, and that the person or persons targeting the home sought its location and/or directions in planning this attack.

(Pet. Exhibit 16, p8).

This analysis did not rely on the fact that the suspects used a cellphone during the crime because the affiant was not seeking devices located in the vicinity of the crime scene (as police would in a geofence warrant). The probable cause determination was based on the theory, supported by historical facts and reasonable inferences therefrom, that the persons who committed this offense had to search for the victims' residence in order to get there to be able to start the fire. This search need not have occurred during the commission of the crime; in fact, there's no reason

it would have been conducted at that point, since the suspects would have already found the residence.

The belief that the suspects would have conducted a search of the victims' address is not based on mere speculation. As explained in the warrant, the house appeared to have been targeted, as it was not a house on a corner with easy access nor did it stand out in this heavily populated neighborhood. In addition, there was no information that would explain why that house, or its occupants would have been targeted; on the contrary, the residents were individuals from Senegal who did not have any known conflict with others who might want to harm them. A reasonable inference from these facts is that the suspects wanted to get to this particular residence but did not already know where it was or how to get there.

Common sense and an understanding of how humans behave when faced with the need for information supports the detectives' reasonable belief that, in order to get to the victims' residence to commit this crime, the suspects would have had to look up the address. Because Google is well known as a ready source of information,[8] and includes an application specific to providing directions (i.e., Google maps), it was

[8] Google is the most frequently used search engine worldwide. *See* https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines

entirely reasonable to expect to find this address search in the records maintained by Google.

"[A] warrant is proper so long as the evidence as a whole creates a reasonable probability that the search will lead to the discovery of evidence." *United States v. Smith*, 266 F.3d 902, 904 (8th Cir. 2001). Under the circumstances outlined above, there was a reasonable probability that the query would lead to the discovery of searches conducted by the suspects who committed the arson/homicide. If the responsive materials, along with any other evidence obtained during the investigation, proved sufficient to establish probable cause that the one or more of the searches were relevant to this offense, additional warrants could be and were obtained to identify the person who conducted those searches.

Seymour complains that searches for the victims' address could have been conducted by persons unconnected to the arson/homicide. This is true. However, probable cause does not require the exclusion of innocent explanations. *See People v. Reyes-Valenzuela*, 392 P.3d 520, 523 (Colo. 2017); *United States v. Fama*, 758 F.2d 834, 838 (2d Cir. 1985) ("The fact that innocent explanation may be consistent with the facts alleged does not negate probable cause."). Moreover, this is the very reason for the staged process used by Google for its keyword and geofence warrants. In either case, it is virtually impossible to identify the exact device/search associated with the

suspect, and the process seeks to identify potential devices or users in the first stage that could belong to the suspect. Once the responsive material from the first stage warrant is provided, the data can be analyzed to rule out and narrow down the pool of devices or users to those potentially relevant. It is only when there is probable cause to believe that the devices or users are relevant to the case (i.e., suspects or direct eyewitnesses) that the identity of the device holders or users is obtained. *See Matter of Search of Info. that is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d at 70-74 (describing geofence process in detail); *Chatrie*, 590 F. Supp. 3d at 914-16 (same).[9]

"The Supreme Court has long recognized and accepted that third party privacy interests could be impacted by lawful searches." *Matter of Search of Info. that is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d at 82 (citing *Zurcher v. Stanford Daily*, 436 U.S. 547, 550 (1978)). "[G]iven the often inherently intrusive task that is evidence gathering, even when performed lawfully by the police—it is neither novel nor surprising that reasonable searches intrude on the privacy interests of individuals who are not the target of criminal investigation." *Matter of Search of Info. that is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d at 84 (citing cases).

> The Fourth Amendment was not enacted to squelch reasonable investigative techniques because of the likelihood—or even certainty—

[9] Seymour's claim that *Chatrie* found that geofence warrants were unconstitutional is incorrect; the *Chatrie* court simply ruled that the warrant *in that case* was invalid. *Chatrie*, 590 F. Supp. 3d at 929.

> that the privacy interests of third parties uninvolved in criminal activity would be implicated. Rather, the Fourth Amendment seeks to ensure that privacy interests are not infringed by law enforcement activities without a showing of probable cause and a particularized description of the place to be searched and the things to be seized.

Id. (internal citations omitted); *see also Matter of Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d at 362 (recognizing that the fact that "uninvolved individuals' privacy rights are indirectly impacted by a search is present in numerous other situations and is not unusual" and "the proper line of inquiry is not whether a search of location data could impact even one uninvolved person's privacy interest, but rather the reasonableness of the search, the probability of finding evidence at the location, and the particularity of the search request").

Also, the potential infringement on third-party privacy interests is minimal (if not completely absent) where, as here, the identity of the persons conducting the responsive searches are not known until the initial responsive results are analyzed, unrelated responses are ruled out, and probable cause is established that the users to be "unmasked" were reasonably believed to have been involved in this case. *See, e.g.*, *Matter of Search of Info. that is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d at 89 ("before any identifying information is disclosed to the government, it must

justify the specific devices for which it seeks that information, consistent with its showing of probable cause").

Seymour's primary challenge to the probable cause determination is this: in order to justify a search of Google's database, which was comprised of the search histories of "billions" of users, Seymour contends that the police had to establish probable cause for each search stored in that database. If that were the case, electronic records contained in any database could never be obtained, unless ISPs maintained separate databases for each user of their services. Seymour's argument is based on his faulty premise that the search here was the functional equivalent of an actual, visual observation of each Google search contained within that database. For the reasons outlined above, this is a mischaracterization of the nature and scope of the search.

Seymour argues that this warrant was invalid because probable cause must be based on individualized facts, not group probabilities, and that law enforcement must have "a reasonable ground for belief of guilt…particularized with respect to [each] person to be searched or seized." *Maryland v. Pringle*, 540 U.S. at 371. More practically, he claims that the warrant should have identified specific accounts and established specific probable cause to search each one, and that it was not enough to believe that evidence existed in some to-be-determined Google account.

First, Seymour's reliance on this body of caselaw in the digital/electronic records context is misplaced. In *Pringle*, as well as in *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979), the Court was addressing a probable cause question related to the physical search or arrest of an individual. In that context, the Court stated, "the belief of guilt must be particularized with respect to the person to be searched or seized." *Pringle*, 540 U.S. at 371.

Here, however, the warrant sought records from an internet service provider based on the belief that one or more of the three known (but not identified) suspects had searched for the victims' address during a brief period prior to the offense. Because the nature of the evidence being sought is different, the nature of the probable cause is necessarily different. The warrant in this case was sufficiently particularized because it sought data related only to specific individuals who conducted a matching search. The fact that the identity of those specific individuals was not known does not contravene the "particularity" or probable cause requirements. *See, e.g.*, *United States v. Besase*, 521 F.2d 1306, 1308 (6th Cir. 1975).

In a case addressing a warrant for use of a canvassing cell site simulator device (CCSS), which functions as a cell tower in order to identify nearby devices in real time, the court found the *Ybarra* analogy, along with the argument that probable cause must be established for each device that connects to the CCSS device, inapplicable

and unwarranted. *In re Warrant Application for Use of Canvassing Cell-Site Simulator*, 2023 WL 1878636, at *11 (N.D. Ill. Feb. 1, 2023). The court reasoned:

> The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, there is a fair probability that contraband or evidence of a crime will be found in a particular place. This standard does not require that the government have probable cause specific to each phone within a CCSS's ambit. The fact that one uninvolved individual's privacy rights are indirectly impacted by a search is present in numerous other situations and is not unusual. Indeed, the Supreme Court has long recognized and accepted that third party privacy interests could be impacted by lawful searches.

Id.; *see also United States v. Smith*, 2023 WL 1930747, at *7 (N.D. Miss. Feb. 10, 2023) (in this geofence case, the defendant similarly argued, relying on *Ybarra*, that the warrant failed to identify and establish probable case for a specific suspect; court found argument unpersuasive).

Again, probable cause requires a fair probability that contraband or evidence of a crime will be found in a particular place. *Illinois v. Gates*, 462 U.S. at 238. Here, the evidence at issue is records of a Google search for the victims' address during the two weeks prior to the arson/homicide. This would certainly constitute "evidence" of a crime because it could reasonably be expected to lead to the identity of one or more of the suspects. *See Matter of Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d at 355 (probable cause where the location data could provide evidence on the identity of the perpetrators and

witnesses to the crime). For the reasons outlined above, it was reasonable to believe that the requested information could lead to the identity of the suspects.

Although Google's query may have yielded unrelated searches, this would not render the search unconstitutional. The identity of those uninvolved individuals would not have been uncovered through this initial keyword warrant, and under the specific terms of this warrant, further judicial involvement would be necessary in order to determine the identity of the persons who conducted the relevant searches.

Ultimately, the touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined by assessing the degree to which it intrudes upon an individual's privacy and the degree to which it is needed to promote legitimate governmental interests. *United States v. Knights*, 534 U.S. at 118-19; *United States v. Montoya de Hernande*, 473 U.S. 531, 537 (1985) ("The Fourth Amendment commands that searches and seizures be reasonable," which "depends upon all of the circumstances surrounding the search or seizure and the nature of the search or seizure itself," and thus "[t]he permissibility of a particular law enforcement practice is judged by 'balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests' ").

Here, the warrant did not constitute an extensive intrusion into the privacy of individuals who conducted Google searches because 1) the search histories contained

in Google's database were not viewed or observed by any human unless they matched the narrow parameters provided and 2) the results of the search were anonymized, thus even the persons who conducted qualifying searches remained private until probable cause to support their unmasking was established. On the other hand, the need for the information was substantial, as a heinous crime had taken the lives of five innocent people (including two very young children) and traditional methods of identifying the suspects had not been fruitful. It simply cannot be said that the search in this case, considering the information known and reasonable inferences therefrom, along with the cautious method by which the search strategy was implemented, was constitutionally unreasonable.

E. The Officers Reasonable Relied on the Warrant in Good Faith.

As demonstrated above, the keyword search warrant was carefully crafted to identify only individuals who may have been involved in this offense and complied with all constitutional requirements for a valid search warrant. However, even if that weren't the case, suppression of evidence obtained from the Google keyword search warrant would not be the proper remedy. Because a warrant was obtained, the good faith rule applies, unless Seymour can establish one of the exceptions to the rule. He has failed to do so.

Section 16-3-308, C.R.S. (2022), creates a presumption that an officer was acting in good faith if he was acting pursuant to a warrant. *People v. Altman*, 960 P.2d 1164, 1168 (Colo. 1998). "The statutory good-faith exception to the exclusionary rule provides that evidence should not be suppressed in a criminal proceeding if it was obtained because of a peace officer's good faith mistake…." *People v. Saint-Veltri*, 935 P.2d 34, 37 (Colo. App. 1996). The ultimate question is whether the officer had a good faith belief in the validity of the warrant, focusing on whether the officer's reliance on the warrant was objectively reasonable. *Altman*, 960 P.2d at 1169. Only when *no reasonable officer* would have relied on the warrant is suppression warranted. *Id.*

There are four circumstances in which an officer's reliance on a warrant would not be objectively reasonable: (1) where the issuing magistrate or judge was misled by a knowing or recklessly made falsehood; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the warrant is so facially deficient that the officers cannot reasonably determine the particular place to be searched or things to be seized; and (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." *United States v. Leon,* 468 U.S. 897, 914 (1984); *Altman*, 960 P.2d at 1170. None of these exceptions apply in this case.

1. False Statements.

Seymour first claims that the good faith rule should not apply because the affiant did not inform the reviewing court of the following "facts": 1) that the warrant would involve the search and seizure of large amounts of unrelated data from "billions" of people; 2) that the promise of "deidentified" data was misleading because the users of the IP addresses could be easily identified; and 3) that two previous warrants for this information had been obtained and withdrawn. He claims that these "material omissions" preclude reliance on the good faith rule.[10]

As demonstrated above, the keyword warrant did not involve a search of "billions" of people. Moreover, nothing in the affidavit or warrant purported to describe the scope of the search or how Google would go about complying with the warrant. And Seymour has failed to provide any legal authority supporting his position that Detective Sandoval was required to do so.

Detective Sandoval also did not include "reckless falsehoods" in the affidavit by "promising deidentified data" would be sought from Google in the first stage of

[10]Notably, these assertions are not "false statements," and Seymour has failed to cite to any caselaw that states that material omissions (as opposed to falsehoods) preclude reliance on the good faith rule. Unquestionably, a warrant itself can be challenged based on material omissions, and the cases cited by Seymour involve material omission claims made in that context. However, he has failed to provide legal authority for his proposition that such omissions can function as "falsehoods" sufficient to constitute an exception to the good faith rule.

the process. The warrant requested two pieces of information: 1) an anonymized list of users who conducted a qualifying Google search; and 2) the IP address associated with each search. Seymour claims that Detective Sandoval knew or should have known that providing the full IP addresses rendered the de-identification of the responsive accounts meaningless. For the reasons described above, this argument must fail.

Third, it is irrelevant that the affidavit did not discuss the previous two applications that were obtained but then withdrawn in an attempt to obtain the keyword information. "An affidavit need not describe all steps taken, information obtained, and statements made during an investigation but must contain any material adverse facts. An adverse fact is material in this context only if its omission would render the affidavit 'substantially misleading as to the existence of probable cause.'" *McKay*, 513 P.3d at 349. The previous steps taken to craft a proper warrant do not constitute "material adverse facts," nor was the omission of any mention of these steps "substantially misleading as to the existence of probable cause" – indeed, they do not bear on anything other than to show the efforts of law enforcement and Google that were taken to ensure that the warrant was constitutionally sound.

Seymour also argues that Detective Sandoval misled the reviewing judge by citing to the Stored Communications Act (18 U.S.C. § 2703) but failing to advise the

judge that the warrant would violate the provisions of the Act. More specifically, he argues that the Act contemplates requests only for data relating to a singular "subscriber," and this warrant sought data related to "billions" of users. However, as recognized in *In re Cell Tower Records Under 18 U.S.C. 2703(D)*, "this argument is effectively refuted by the Dictionary Act, which instructs courts that '[i]n determining the meaning of any Act of Congress, unless the context indicates otherwise, words importing the singular include and apply to several persons, parties or things; [and] words importing the plural include the singular....'" 90 F. Supp. 3d 673 (S.D. Tex. 2015) (citing 1 U.S.C. § 1); *see also United States v. Pendergrass*, 2019 WL 1376745 (N.D. Ga. 2019); *In re Application of the United States of America*, 42 F. Supp. 3d 511, 513 (S.D.N.Y. 2014).

2. Facial deficiency.

Seymour next contends that the warrant was so facially deficient that no objective officer could reasonably presume it was valid. However, he fails to describe what aspects of the warrant were "facially deficient." This exception applies where the warrant is such that the officers cannot reasonably determine the particular place to be searched or things to be seized. *Altman*, 960 P.2d at 1169. To the contrary, the warrant here was directed at Google, to be executed by Google, and was very specific as to the information being sought. As such, this exception was not established.

3. "Bare Bones" Affidavit.

Last, Seymour argues that the keyword warrant was "so lacking in indicia of probable cause" that it was entirely unreasonable for an officer to rely on it. This is known as a "bare bones" affidavit. Seymour claims that "the government simply assumed that a cell phone was involved, and that Google had relevant data."

As noted above, this is not a geofence or tower dump warrant and as such, probable cause is not dependent upon the simple presence of a suspect with a cellphone at the crime scene. Probable cause was based on the notion that, under the totality of the circumstances, it was reasonable to believe that someone unfamiliar with the victims nevertheless targeted their residence, and that they likely would have been required to search for the residence in order to get to it. These assertions were supported by the information obtained during the investigation, including physical evidence (i.e., the location of the residence and the characteristics of the neighborhood) and details observed in the various surveillance recordings. It cannot be said that the affidavit contained "wholly conclusory statements devoid of facts from which a magistrate can independently determine probable cause." *Altman*, 960 P.2d at 1170.

The People do not dispute that this warrant was novel and that no caselaw exists addressing this type of search or the language that should appear in a Google

keyword search warrant. Detective Sandoval consulted with the District Attorney's Office during the process of crafting the warrant and worked with Google to ensure that the language included in the warrant satisfied Google's requirements as well as those of the United States and Colorado Constitutions. *See United States v. McLamb*, 880 F.3d 685, 691 (4th Cir. 2018) ("[I]n light of rapidly developing technology, there will not always be definitive precedent upon which law enforcement can rely when utilizing cutting edge investigative techniques. In such cases, consultation with government attorneys is precisely what *Leon*'s 'good faith' expects of law enforcement. We are disinclined to conclude that a warrant is 'facially deficient' where the legality of an investigative technique is unclear and law enforcement seeks advice from counsel before applying for the warrant."). Suppression is not warranted here.

CONCLUSION

For the above reasons, the district court's order should be upheld, and the Rule to Show Cause should be discharged.

Date: March 7, 2023.

Respectfully submitted,
BETH MCCANN
Denver District Attorney

/s/ Katherine A. Hansen
KATHERINE A. HANSEN
Senior Deputy District Attorney

JOSEPH M. MORALES
Chief Deputy District Attorney

COURTNEY L. JOHNSTON
Chief Deputy District Attorney

CERTIFICATE OF SERVICE

I certify that on March 7, 2023, I e-filed the foregoing via CCE, which will notify all counsel of record.

/s/ Katherine A. Hansen