DISTRICT COURT, DENVER COUNTY, COLORADO 520 W. Colfax Denver, Colorado 80204	DATE FILED: June 30, 2022 12:03 PM FILING ID: 2D0BFA23AF560 CASE NUMBER: 2021CR20001
PEOPLE OF THE STATE OF COLORADO, Plaintiff, v. GAVIN SEYMOUR, Juvenile Defendant.	▲ COURT USE ONLY ▲
JENIFER STINSON (#35993) Stinson Law Office 1245 E. Colfax Avenue, Suite 300 Denver, Colorado 80218 Phone: (303) 483-3161 E-mail: JStinsonLaw@gmail.com MICHAEL S. JUBA (#39542) Juba Law Office, PLLC 675 N. Grant Street Denver, CO 80203 Phone: (303) 974-1080 E-mail: Juba@JubaLawOffice.com MICHAEL W. PRICE (#22PHV6967) National Association of Criminal Defense Lawyers 1660 L Street NW, 12th Floor Washington, DC 20036 Phone: (202) 465-7615 E-mail: MPrice@NACDL.org	Case Number: 21CR20001 Division: 5A
MOTION TO SUPPRESS EVIDENCE FROM A KEYWORD WARRANT & REQUEST FOR A VERACITY HEARING	

INTRODUCTION

Gavin Seymour, through counsel, moves to suppress all evidence and its fruits derived from a modern-day general warrant: a reverse Google keyword search in violation of the Fourth Amendment of the United States Constitution and Article II, Section 7 of the Colorado Constitution. U.S. Const. amend. IV; Colo. Const. art. II, § 7. Relatedly, Mr. Seymour moves for

a veracity hearing to establish that the warrant affidavit substantially misled the issuing judge. As grounds, Mr. Seymour states as follows:

1. A reverse keyword search is a novel and uniquely intrusive digital dragnet of immense proportions. It requires Google to search billions of people's search queries—everyone who ran a Google search—and produce information on anyone who looked for certain search terms, or keywords. Here, the government searched for, and then seized, the personal data associated with everyone who searched for nine variations of an address, "5312 Truckee Street," over the course of 15 days in 2020. *See* Attachment 1 (Nov. 19 Keyword Warrant) at 2656.[1]

2. But for this reverse keyword search, law enforcement would not have identified Mr. Seymour as a suspect in this case. Indeed, the keyword warrant was preceded by a litany of other constitutionally suspect searches. None of them, however, pointed law enforcement to Mr. Seymour. In fact, the operative keyword warrant, issued on November 19, 2020, was the third keyword warrant issued in this case. *See* Attachment 2 (Oct. 1 Keyword Warrant); Attachment 3 (Oct. 20 Keyword Warrant). Google refused to comply with the first two. And just the day before Denver police obtained the warrant, investigators were interrogating an alternate suspect. 11/12/21 Tr. ("Prelim. Tr.") at 72–73. Law enforcement went on a massive fishing expedition, trawling through everyone's cell phone records, location data, and Google data—without cause to search any of it—until they identified Mr. Seymour with a third keyword warrant.

3. No court has considered the legality of a reverse keyword search, but its constitutional defects are readily apparent and should have been obvious to all involved. It is a 21st century version of the general warrants that the Fourth Amendment was designed to guard against. Just as no warrant could authorize the search of every home in America, no warrant can compel a search of everyone's Google queries.

4. Everyone, including Mr. Seymour, has a Fourth Amendment interest in their internet search history, which contains an archive of intimate personal expression. Search engines like Google are a gateway to the vast trove of information online, and the only way most people can find what they are looking for online. Even a single query can reveal deeply private facts about a person, things they might not share with friends, family, or clergy: "psychiatrists in Denver;" "abortion providers near me;" "is my husband gay;" "does God exist;" "bankruptcy;" "herpes treatment." Yet everyday people pose these queries to Google in pursuit of answers, information, and advice. Stitch the searches together over time and they form a tapestry of daily life, woven from a person's worries, questions, and secrets. Search history is a window into what people wonder about—and it is some of the most private data that exists.

5. Mr. Seymour did not consent to having his Google data searched, and the so-called "third-party doctrine" is inapplicable. Search queries are fundamentally different from the business records to which the third-party doctrine traditionally applies. *See Smith v. Maryland*, 442 U.S. 735 (1979) (numbers dialed on a landline); *United States v. Miller*, 425 U.S. 435 (1976) (bank deposit slips). Instead, they reveal information that is even more private than the seven days of cell phone location data that the Supreme Court found were constitutionally protected in

[1] All references to the attachments in this motion cite to the Bates numbers provided on those documents, where available.

Carpenter v. United States. 138 S. Ct. 2206 (2018). Moreover, Google is no ordinary third party: "Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible." *Id.* at 2219. Indeed, records of Google search queries are comprehensive and inescapable, captured with every query, from every user, regardless of whether they are signed in to a Google account. *See* Attachment 4 (Declaration of Nikki Adeli) ¶ 14. And because each query is tied to a unique ID number as well as the Internet Protocol ("IP") address assigned to each user, they are personally identifiable.

6. The government searched an ocean of intensely private data in this case, yet it lacked probable cause to search even one Google user. Instead, it demanded that Google search *everyone's* Google searches in order to generate suspicion. This process is profoundly different from the one that governs the application for and execution of typical warrants, where a suspect is known and the warrant seeks their data. Instead, this "reverse warrant" first identifies categories of data and then seeks information about people whose data falls into those categories.

7. The warrant therefore violates the Fourth Amendment and the Colorado Constitution for lack of probable cause and particularity. It is unconstitutionally overbroad and unparticularized, the digital equivalent of a general warrant, and all evidence obtained or derived from it must be excluded as the fruits of an unconstitutional search. *See Mapp v. Ohio*, 367 U.S. 643 (1961). Furthermore, no reasonable officer could have believed that such a warrant was valid. The government was desperate to make an arrest, and it sought a warrant with impermissibly broad discretion to search and seize data about unspecified people. It therefore violated the Fourth Amendment and cannot be saved by the good-faith exception.

FACTS

I. A Pattern of Dragnet Searches

8. This case turns on the third reverse keyword warrant that the Denver Police Department served on Google, requiring the search of billions of people. It is undoubtedly one of the broadest searches in Fourth Amendment history. But it was also part of a pattern of increasingly invasive and boundless searches affecting the privacy rights of countless people with no connection to this case. The police, working with the federal Bureau of Alcohol, Tobacco, Firearms, and Explosives, sought a stunning array of warrants seeking the private data of anyone and everyone who was within at least a mile of the area.

9. Prior to the third keyword warrant, the government executed at least 23 other warrants, escalating over time to "very general search warrants" without any named suspects. Prelim. Tr. at 66; *id.* at 61–62 (acknowledging that law enforcement obtained "search warrants to search kind of general areas" for "[w]ho may have been in the general area at a specific time"). These included two "tower dumps", Prelim. Tr. at 67–68, 70–71, 122–25, 139 162–64, 178–79, 191; and the use of one "cell-site simulator" (a.k.a. "IMSI catcher"), *id.* at 127–28. Tower dumps seek "information on every single device that had connected to [cell] towers in the area," implicating "thousands of people's phone numbers" or "hundreds of different people that lived in the area." *Id.* at 70–72, 81; *see also id.* at 123–24, 164. These warrants searched and seized information pertaining to devices that belonged to "thousands of people," *id.* at 71, all without identifying a suspect. Here, when police requested a "traditional tower dump" and

"specialized location data dump," *see id.* at 123–24, from four major cell phone carriers, one returned 1,471 "unique devices…within a 1-mile radius" of the fire, *id.* at 125, and another returned 4,595 devices, *id.* at 126.

10. None of this information led investigators to identify a suspect. But to try and make sense of it all, they obtained even more information. Police deployed a "cell-site simulator" (a.k.a. "IMSI catcher") in the same neighborhoods in an attempt to "throw out" some numbers. *Id.* at 128. A cell-site simulator is a fake cell phone tower operated by the police from the back of a car. *See id.* at 127–128. As the police drove the device around Truckee St. on August 20, 2020 at 2 a.m., the simulator forced every cell phone within range to connect to it instead of to the authentic cell phone network. The phones then identified themselves to the police by providing their unique international mobile subscriber identifier ("IMSI") numbers. *Id.* at 127. Police identified 723 devices in the area, most of which belonged to neighbors in private homes. *Id.* at 128–129. None of this information, however, led investigators to say, "We've got our guy or gal or anything." *Id.* at 129.

11. Police also obtained two Google geofence warrants, one on August 10, 2020, and another on October 6, 2020. *See* Attachment 5 (Aug. 10 Geofence Warrant); Attachment 6 (Oct. 6 Geofence Warrant). A geofence warrant is a type of reverse warrant that searches all Google users with "Location History" enabled for all devices in a given area. *See also United States v. Chatrie*, No. 3:19-CR-130, 2022 WL 628905, at *3–4 (E.D. Va. Mar. 3, 2022) (finding a geofence warrant unconstitutional). Google maintains this data on "numerous tens of millions" of users. *Chatrie*, 2022 WL 628905, at *3. For reference, Google had 592 million Location History users in 2018. *See* Attachment 7 (Declaration of Emily Moseley) ¶ 3. To conduct a geofence search, regardless of the size or shape of the area, Google must comb through the account of every Location History user. *Chatrie*, 2022 WL 628905, at *9. That is because Google does not know which users may have responsive data before conducting the search. *Id.* As a result, the two geofence warrants here, covering six geographic areas, led to the search of hundreds of millions of people, multiple times. Yet, like the prior searches, this approach also failed to produce any "fruitful" leads. Prelim. Tr. at 47.

12. Additionally, the police obtained a warrant to access and receive information from a company named "Fog Data Science" via the "Fog Reveal Portal." *See* Attachment 8 (Fog Data Warrant) at 1454. Fog Data Science is a private company that aggregates device location information from different databases and online sources to sell that information to others. *Id.* at 1457. The information is linked to "Advertising ID" generated by individual devices, as well as a unique device identifier assigned by Fog. *Id*. Much like a Google geofence warrant, the Reveal Portal allows police to search Fog's database to locate devices that were present in an area during a given time. Investigators may identify "devices of investigative interest" and then run a "device specific query…for a duration of time over an unconstrained geographical area." *Id.* at 1458. Fog collects "more than 15 billion signals globally" each day. *Id.* at 1457. The search here covered two areas over a total of 45 minutes, *id.* at 1454–55, resulting in the search of hundreds

of millions of records held by Fog. Once again, however, it did not produce any "fruitful" leads.[2] Prelim. Tr. at 47.

13. Only one search warrant produced information that led police to identify Mr. Seymour as a suspect in this case—the third keyword warrant, issued on November 19, 2020. *See* Attachment 1 (Nov. 19 Keyword Warrant); Prelim. Tr. At 47. This was the broadest dragnet by far, resulting in the search of billions of Google users.

II. Reverse Keyword Warrants Generally

14. Reverse keyword warrants are a new type of search. They are unlike anything courts have approved in the past, and they are antithetical to both the Fourth Amendment and the Colorado Constitution. No keyword warrant has been tested in an adversarial proceeding, and there are no reported decisions concerning their constitutionality. Thus, until now, not much has been known about how Google executes keyword warrants.

15. In this case, Google has provided a declaration describing, for the first time, how a reverse keyword search works. *See* Attachment 4 (Declaration of Nikki Adeli). As a threshold matter, Google requires law enforcement to obtain a warrant. *Id.* ¶ 3. That is because Google treats search query data as private content belonging to individual Google users. *See* Attachment 9 (Google Privacy Policy) at 22. Google keeps a record of every search query that users make. If a Google user is signed-in to their account, then their search queries are logged and saved to their account, which is personally identifiable by a "GAIA ID" ("Google Accounts and ID Administration") number. Attachment 4 (Declaration of Nikki Adeli) ¶ 14. If a user is not signed-in or does not have a Google account, then Google assigns a "Browser Cookie ID" number based on the individual characteristics of the computer involved. *Id.* ¶ 7. Both the GAIA ID and the Browser Cookie ID are personally identifiable with information available to law enforcement with a subpoena. And in both cases, Google also retains the user's IP address, which law enforcement can use to subpoena subscriber information, including names and addresses. *See id.*

16. Google asserts that it "generally" uses a "staged process" for executing keyword warrants. *Id.* ¶ 3. During the first stage, upon receiving a keyword warrant, Google "creates a text-based query []that can include letters, numbers, or characters" based on the keyword search terms identified in the warrant. *Id.* ¶ 4. That query is "run over the records of searches conducted through Google Search and Maps." *Id.* This includes searches conducted by "authenticated" (logged-in) Google users as well as searches from users who are not authenticated. *See Id.* ¶ 7. Put another way, when responding to a keyword warrant, Google searches all queries run on Google Search or Google Maps, regardless of whether the person who conducted the search was logged into a Google account or consented to such use of their Google Search or Maps histories. As Google acknowledges, at the point the warrant is executed, there is no way to know which users—if any—have used the keywords contained in the warrant. *Id.*

[2] It remains unclear to the defense whether use of the Fog Reveal Portal produced no results, or whether the government did not retain a record of its search results. The Denver Police Department and the ATF both have paid subscriptions to the Fog Reveal Portal. *See* Attachment 8 at 1457.

17. This process yields a set of raw results that reflect who searched for the terms identified in the warrant. *Id.* Google then makes certain decisions about what information to include in its production to law enforcement. *See id.* ¶¶ 7–8. Google decides, for instance, whether to "limit the results to queries that contain only the search terms listed in the warrant and no other words," or, "more commonly," produce results that contain additional words or terms not specified in the warrant. *Id.* ¶ 6 (e.g., "1600 Amphitheater Parkway" vs. "1600 Amphitheater Parkway Google Headquarters"). It will do so even where the search results strongly imply that a keyword search is irrelevant. *See id.* ¶ 8 (stating that Google will disclose search results for similar addresses in other cities or states).

18. Before turning over the query results to law enforcement, Google may "de-identif[y]" the results. *Id.* ¶ 8. The "production version" of the query results "typically includes the following categories of information: (1) the date and time of the [keyword] search, (2) coarse location information inferred from the IP address from which the search was conducted, (3) the Query…, (4) the Result…, (5) the Host…, (6) the Request…, (7) a truncated Google identifier (known as the GAIA ID), if the search was conducted from an authenticated user's account, or a truncated version of a Browser Cookie ID if the search was not conducted from an authenticated user's account and (8) the associated user agent string." *Id.* ¶ 7. The "Query" is the search query a user enters into Google Search or Google Maps. *Id.* ¶ 4. The "Result" refers to the "result generated by Google from a user's queried search." *Id.* ¶ 7. "The Host" is "the Google domain name that the user contacted (e.g., google.com and google.fr.)." *Id.* The "Request" is the latter part of the same URL and it distinguishes between user-generated searches an "background requests made of Google's servers" ("GET" vs. "POST"). *Id.* The GAIA ID is a unique number associated with each Google account. And a "Browser Cookie ID" is a unique number associated with the web browser that conducted the search. *Id.*; *see also* Attachment 9 (Google Privacy Policy) at 23.

19. While Google asserts that it de-identifies these results before disclosing them to law enforcement, *see id.* ¶ 3, the information provided can be used to identify people who used the relevant search terms without additional court supervision. As Google explains, during the second stage of executing the warrant, law enforcement "can compel Google to provide additional information for those users the government has determined to be relevant to its investigation" if allowed by the warrant. *Id.* ¶ 9. Separate from this, law enforcement can use a subpoena to obtain the name and address of the account holder. *See id.* ¶ 9 (stating that law enforcement can use subpoenas under 18 U.S.C. § 2703(c)(2) to obtain various categories of identifying formation after determining which accounts are relevant to the investigation). There is nothing in Google's process that prevents law enforcement from seeking identifying information about all users in the de-identified query results.

20. Importantly, Google does not follow this process in all cases. Rather, Google qualifies that it "generally" uses the staged process described, *id.* ¶ 3, but in some cases—like this one—Google deviates significantly. As detailed below, the November 19 keyword warrant explicitly compelled Google to disclose full IP addresses in "stage one," making it meaningless to "de-identify" other information like the full GAIA or Browser Cookie IDs. Law enforcement can and did use the IP addresses provided to identify Google users, including Mr. Seymour.

III. The Three Keyword Warrants in This Case

21. With no leads in their investigation, investigators determined they "were going to write a search warrant to Google to see if there[] [were]…any keyword searches for the address" where the fire occurred. Prelim. Tr. at 47. The warrant would require Google to determine which, if any, users had searched for nine variations of the address (accounting for different spellings like "North" versus "N.," or "Street" versus "St.") "to see if anybody would have Googled that address…prior to the fire." *Id.* Google, however, rejected the first two such keyword warrants, only complying with the third after directing investigators on the language it wanted included. *See* Attachment 10 (Supplementary Report) at 3760. The three keyword warrants all focused on the same address over the same 15 days, but they differed significantly in the types of data to be produced and the process for obtaining it from Google.

A. The First Keyword Warrant

22. On October 1, 2020, the government submitted the first keyword warrant to Google. The October 1 warrant requested data about users who searched for nine variations of "5312 Truckee Street"[3] over the course of 15 days ("July 22, 2020 at 00:01 M.S.T. through and to include August 5, 2020 at 0245 M.S.T."). *See* Attachment 2 (Oct. 1 Keyword Warrant) at 3138–39. It had just one step. Specifically, for each responsive query, the warrant required Google to produce "the personal identification of the subject account, to include full name, date of birth, email address(es), physical address(es), and telephone numbers." *Id.* at 3139. Google refused to comply with this warrant and escalated the matter to outside counsel at Perkins Coie LLP. Through counsel, Google emailed investigators on October 15, 2020, to state that the search warrant needed to be revised.[4] *See* Attachment 10 at 3757. According to Google, the warrant did not comport with its required de-identification procedures, presumably because it called for Google to produce full names and addresses for all responsive queries. *See* Attachment 4 (Declaration of Nikki Adeli) ¶ 11.

B. The Second Keyword Warrant

23. On October 20, 2020, the government submitted a second keyword warrant to Google. *See* Attachment 3. Like the first warrant, the October 20 warrant used the same nine variations of the "5312 Truckee Street" address and involved the same 15-day timeframe, between July 22, 2020, and August 5, 2020. *Id.* at 2659–60. This second version, however, sought "anonymized information" for responsive queries, meaning that Google would produce an "Anonymized List" of responsive devices with "an identifier assigned by Google…which does not contain any unique device identifier/individual account identifier." *Id.* at 2660. Law enforcement would then "review the Anonymized List to remove device IDs that [were] not relevant" and

[3] Specifically, the warrant sought information about everyone who had searched for one or more of the following terms: "5312 Truckee"; "5312 Truckee St"; "5312 Truckee Street"; "5312 N Truckee St"; "5312 N. Truckee St."; "5312 N. Truckee St"; "5312 N Truckee St."; "5312 North Truckee"; "5312 North Truckee Street".

[4] The government has not produced this communication to the defense despite multiple requests. The defense still does not know how Google counseled investigators to revise the first warrant.

create a "shortlist" from the Anonymized List. *Id*. If they wanted "additional information…that [fell] outside of the Initial Search Parameters," they would provide a "subsequent warrant." *Id.* Indeed, this warrant explicitly provided that "[l]aw enforcement shall not seek or be provided any further subscriber/device information unless an additional search warrant is obtained." *Id.* at 2661.

24. Despite the revised process, however, this second keyword warrant included a new, additional demand for user location data, which Google treats as account content. Unlike the first warrant, the second one required Google to produce two days of location data (August 4–6, 2020) for each account identified as responsive to the keyword search. *Id.* at 2660. In effect, it was a keyword search combined with a geofence search. It also contradicted the warrant affidavit—essentially a copy of the first—which promised that "[n]o other contents of the account are being sought at this time." Attachment 3 at 3068. And once again, Google did not comply. On October 30, 2020, Google's outside counsel at Perkins Coie called investigators and "advised that again the language in the search warrant was not correct and the search warrant again would need to be revised." Attachment 10 at 3759.

C. The Third Keyword Warrant

25. On November 17, 2020, investigators had another phone call with Google's outside counsel, this time "to work out the language that [Google] would like in the warrant." Attachment 10 at 3760. The Denver District Attorney was invited to join. *See* Attachment 11 (Email with Hayley Berlin) at 6110–13. The defense still does not have a record of who participated, what transpired, or how Google directed law enforcement to draft the warrant, but on November 19, 2020, the government submitted a third and final keyword warrant to Google. *See* Attachment 1 (Nov. 19 Keyword Warrant) at 2656–58. This warrant differed from the first two in a critical way: it required Google to provide full IP address information for every responsive search query.

26. The third keyword warrant again sought returns for the same nine variations of the address where the fire occurred and same 15-day timespan for those searches. *See id.* at 2656. It did not request any location information, and instead asked for "anonymized information" responsive to the keyword search. *Id.* at 2657. But significantly, it also demanded "the IP addresses used by all accounts that are found to have conducted" one of the keyword searches. *Id.*

27. Including IP addresses is significant because they are *not* anonymous identifiers. Police routinely use this information to identify individuals responsible for online activity. An IP address is required for any device to access the internet, including Google, and it is assigned by internet service providers, like Comcast. *See* Prelim. Tr. at 133. Service providers maintain records of which IP addresses were assigned to which customers at what times. And they also maintain subscriber, payment, and street address information for those customers. As a result, law enforcement can easily associate an IP address with a particular subscriber or street address. *See id.* at 133–34 ("An IP address is essentially…a value that is used to identify a device on a network. As far as investigations go, we can…figure out where that IP address was utilized or…the subscriber of the account related to the usage of that IP address."); *see also*

Attachment 12 (Comcast Warrant), Attachment 13 (AT&T Warrant); Attachment 14 (Verizon Warrant); Attachment 15 (T-Mobile Warrant).

28. Google also recognized the significance of including full IP addresses, which is why their keyword warrant procedure did not allow for the disclosure of that information. *See* Attachment 4 (Declaration of Nikki Adeli) at ¶ 7. Instead, Google's policy was to include only "coarse location information inferred from the IP address from which the search was conducted" in the initial "production version." *Id.* In this case, however, Google did not follow that policy. *Id.* at ¶¶ 13–15. Instead, it complied with the third keyword warrant as written.

29. Consequently, Google searched billions of users—worldwide—and produced two spreadsheets containing a total of 61 queries that it deemed responsive. *See* Attachment 16 (Keyword Warrant Return Data). The government has testified that the search was limited to the entire state of Colorado, *see* Prelim. Tr. at 82 ("I believe we limited it to Colorado"), but this is incorrect.[5] The spreadsheets returned by Google include a list of states ("Subdivisions") associated with each IP address. Of the 61 queries, 38 were associated with Colorado; 2 were associated with Illinois; and 21 were blank. *See* Attachment 16. The government also acknowledged in a subsequent search warrant that the "information provided…was for any account where the states IP address were resolved." *See* Attachment 17 (Dec. 4 Google Warrant) at 2612.

30. Moreover, most of the queries Google returned did not match any of the nine variations "5312 Truckee St." specified in the warrant. Only five did. Instead, there were 45 that contained additional search terms, such as state, zip code, or the word "interior." And there were another 11 entries that did not specify the search query used at all, leaving that field entirely blank.

31. Still, Google provided either a truncated GAIA or Cookie ID for each of the 61 queries, depending on whether the user was signed-in to their account at the time. *See* Attachment 16. There were five distinct GAIA IDs and four distinct Cookie IDs, suggesting that the data seized belonged to up to nine people.[6] *Id.* Critically, Google provided full IP addresses for 60 of the 61 queries, leaving one filed blank. *Id.; see also* Prelim. Tr. at 132, 135 (stating that the return included IP addresses). There were 12 distinct IP addresses responsible for those 60 queries,

[5] The government limited subsequent search warrants to the five Google accounts with IP addresses resolved to Colorado, as described *infra*, but it received data on at least four others.

[6] The government has testified that Google provided five "accounts" in response to the keyword search warrant. Prelim. Tr. at 192. But the presence of four additional Cookie IDs, with no associated GAIA IDs, indicates that other people may have run responsive queries while not logged-in to a Google account. *See* Attachment 18 (Report of Investigation No. 7) at 5843 ("Responsive data from Google indicated *at least* five users who…quer[ied] that address") (emphasis added); *see also* Prelim. Tr. at 196 ("What we were able to determine is that someone was using a Google product to search that address but was not logged into a Google account at that point in time. So, when that address was queried, Google obviously knew that that address was queried, but they could not attribute it back to a Google user because it -- whoever it was at that point was not logged in.").

indicating that at least two of the nine people had searched Google from more than one IP address. *See id*.

IV. Subsequent Investigation

32. Based on Google's return from the third keyword warrant, investigators focused on the five Google accounts with IP addresses in Colorado. *See* Attachment 17 at 2612; Prelim. Tr. at 131. They also saw that three accounts had searched for the Truckee Street address multiple times, some of which raised "red flags" because they included the word "interior." Prelim. Tr. at 48. Consequently, on December 4, 2020, investigators obtained five additional warrants seeking subscriber information associated with that activity. *See id.* at 135; Attachment 18 (Report of Investigation No. 7) at 5843.

33. One warrant required Google to produce subscriber information, in addition to all account contents, for all five accounts. *See* Attachment 17 at 2604–05. Google refused to produce the account contents. *See* Attachment 4 (Declaration of Nikki Adeli) ¶ 16 ("Google objected to the warrant to the extent it required disclosure of content or other records based on a truncated GAIA ID and advised that new legal process would be required to obtain additional information."). But it did produce the subscriber information, which showed that one account belonged to Mr. Seymour. *See* Attachment 18 (Report of Investigation) at 5843.

34. The other four warrants required various internet service providers—Comcast, AT&T, Verizon, and T-Mobile—to produce subscriber information associated with the full IP addresses in the keyword search return. Attachment 12 (Comcast Warrant) at 3040–41, 3049–50; Attachment 13 (AT&T Warrant) at 3037; Attachment 14 (Verizon Warrant) at 3191; Attachment 15 (T-Mobile Warrant) at 2698. Comcast complied, stating that two of the accounts were registered to "Stephanie Johnson" at an address in Lakewood, CO. *See* Attachment 20 (Comcast Warrant Return) at 2775. Ms. Johnson is Mr. Seymour's mother, and they lived together at the same address in Lakewood.[7]

35. Based on this information, law enforcement obtained further warrants to search Mr. Seymour's full Google account, as well as his Snapchat, Facebook, Instagram, and Apple iCloud accounts. *See* Attachment 21 (Google Account Warrant) at 5967–6088; Attachment 22 (Snapchat Account Warrant) at 4276–77; Attachment 23 (Facebook & Instagram Account Warrant) at 4245–49; Attachment 24 (Apple iCloud Account Warrant) at 5492–539. The government also obtained Mr. Seymour's text messages and historical cell phone location information. *See* Attachment 25 (AT&T Call Detail Warrant) at 2862–64. And after reviewing this information and conducting further investigation, police arrested Mr. Seymour on January 27, 2021. But for the keyword warrant, however, investigators would have never identified Mr. Seymour as a suspect in this case, let alone obtained his account contents and arrested him. *See* Prelim. Tr. at 50–51.

[7] Comcast stated that the third IP address was registered to Tanya Bui, the older sister of co-defendant Kevin Bui. *See* Attachment 20 at 2777. The related search query was not conducted from an authenticated Google account, however. As a result, there was no GAIA ID provided, only a truncated Cookie ID.

ARGUMENT

36. The November 19 keyword warrant authorized a Fourth Amendment search. It was a search because it violated Mr. Seymour's reasonable expectation of privacy in his Google search query history and because it infringed on Mr. Seymour's property rights in his Google account data. Critically, it was not just a search of Mr. Seymour, but a search of billions of Google users, and all without a shred of evidence to search any one of them. In short, it was an unconstitutional general warrant.

37. Because this search also implicates the First Amendment, courts must apply the Fourth Amendment's requirements with "the most scrupulous exactitude." *Stanford v. Texas*, 379 U.S. 476, 485 (1965). Indeed, the Colorado Supreme Court has held that the First Amendment to the United States Constitution and Article II, Section 10 of the Colorado Constitution protect an individual's right to obtain information anonymously, and that the government must meet a higher burden to get a search warrant for such records when they are maintained by a third-party. *See Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1047 (Colo. 2002) (involving a warrant authorizing the seizure of customer purchase records from a bookseller). The government must demonstrate "a compelling governmental need" for the "specific" records they seek, considering whether there are "reasonable alternative methods" of investigation, whether the warrant is "unduly broad," and whether the records are sought for "reasons related to the content" of the information at issue. *Id.* The keyword warrant here failed to meet this heightened standard. Indeed, the warrant was fatally overbroad and profoundly lacking in particularity. It did not demonstrate probable cause to search and seize *anyone's* Google data, let alone cause to search billions of accounts. And it lacked particularity because it failed to specify which accounts could be searched and seized, enabling the government to act far beyond the scope of a proper search.

38. Finally, the good-faith exception does not apply to the instant keyword warrant because the affidavit omitted critical facts and substantially misled the issuing judge. The warrant also lacked sufficient indicia of probable cause and was facially deficient. No reasonable officer would believe that a dragnet search of every home in America is constitutional. And there is no good reason to think that it would be permissible in the digital sphere.

I. A search of Google queries is a Fourth Amendment search.

39. In *Carpenter v. United States*, the Supreme Court found that law enforcement's acquisition of cell site location data constituted a search. 138 S. Ct. at 2220. The Court ruled that individuals have an expectation of privacy in their location data, even when it is held by a third-party service provider. *Id.* Because keyword search data is even more revealing than cell phone location data, law enforcement must also get a warrant to search it under *Carpenter*. Furthermore, an individual's Google account data, including their search history, is their private property. It is the digital equivalent of the "papers" and "effects" that are explicitly protected by the Fourth Amendment and the Colorado Constitution. U.S. Const. amend. IV; Colo. Const. art. II, § 7. As such, a search of Google account data is also a trespass because it infringes on the user's property rights, and it is therefore a Fourth Amendment search requiring a warrant.

A. People have a reasonable expectation of privacy in their keyword search information.

40. The Fourth Amendment protects people from unreasonable searches and seizures of things in which they have a reasonable expectation of privacy. *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring). Individuals have a reasonable expectation of privacy when (1) a person has exhibited an "actual (subjective) expectation of privacy," and (2) that the expectation is "one that society is prepared to recognize as 'reasonable.'" *Id.* at 361 (Harlan, J., concurring).

41. The U.S. Supreme Court has recently clarified how to identify a reasonable expectation of privacy in the digital context. Courts should look to "historical understandings" of what was unreasonable at the nation's founding, guided by the understanding that the Fourth Amendment (1) aims to secure "the privacies of life" and (2) "place obstacles in the way of a too permeating police surveillance." *See Carpenter*, 138 S. Ct. at 2214. The Court has sought to preserve a "degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo v. United States*, 533 U.S. 27, 34 (2001). Consequently, the Court considers whether the "retrospective quality" of the data gives the government access to a category of information that would be "otherwise unknowable" before the digital age. *Carpenter*, 138 S. Ct. at 2218; *see also Riley v. California*, 573 U.S. 373, 393–94 (2014); *People v. Tafoya*, 494 P.3d 613, 623 (Colo. 2021) (holding that three-month-long surveillance of a home using a pole camera violated the Fourth Amendment following *Carpenter*).

42. Keyword data reveals the privacies of life by exposing what people wonder, desire, believe, and fear. *See* Seth Stephens-Davidowitz, *Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us About Who We Really Are* 3 (2017). It can show that someone hates their boss, is the victim of domestic abuse, is unhappy in their marriage, or was recently diagnosed with cancer. *See id.* at 6, 27. These are intimate details that paint intimate portraits of the inner workings of people's minds, and people want and expect this information to remain private.

43. In many ways, this information is even more revealing than the location data at issue in *Carpenter*. There, the Court held that cell-site location information ("CSLI") revealed "privacies of life" to law enforcement because a cell phone "tracks nearly exactly the movements of its owner" as they travel "into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *See Carpenter*, 138 S. Ct. at 2217–18. Keyword search data exposes more personal information. Instead of merely tracking a visit to the doctor, keyword search data can expose a person's medical diagnosis. Instead of following a person to a "potentially revealing" location, keyword search data explicitly reveals a person's thoughts about any number of topics including things like race relations in the United States or their sexual orientation. *See* Stephens-Davidowitz, *supra*, at 6, 117. CSLI gives the government dots on a map which enables it to make inferences about "familial, political, professional, religious, and sexual associations." *See United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). By contrast, keyword search data gives the government explicit information about an individual's innermost thoughts and associations. Brennan Ctr. for Justice, *Applying the Supreme Court's* Carpenter *Decision to New Technologies* 4 (Mar. 18, 2021), https://perma.cc/JK3J-C9N2.

44. Additionally, keyword search data reconstructs information that would have been unknowable in 1791, when the Fourth Amendment was ratified. In *Carpenter*, the Supreme Court highlighted that the precision and scale of CSLI surveillance would have been impossible when the Fourth Amendment was adopted. *See Carpenter*, 138 S. Ct. at 2218. Similarly, an analysis of Google search terms retrospectively reveals information about a person that would otherwise be unknowable to police. A person's search history is an inventory of all the names, addresses, and subjects about which they sought information. At the time the Fourth Amendment was adopted, this information would have been impossible to collect.

45. Mr. Seymour had a reasonable expectation of privacy in his keyword search data because it contains the "privacies of life" and because it reflects information that would have otherwise been unknowable to law enforcement. A search of this information is the epitome of a "too permeating police surveillance." *Id.* at 2214 (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)). This warrant authorized a Fourth Amendment search.

B. The third-party doctrine does not apply to Google search data.

46. Mr. Seymour did not voluntarily convey his keyword search data to Google in any meaningful way, and thus did not waive the privacy interest he had in his keyword search data.

47. The third-party doctrine is an exception to the Fourth Amendment that allows law enforcement to warrantlessly search information that a person voluntarily conveys to a third party. The Supreme Court crafted this doctrine in the 1970s in the context of bank deposit slips and telephone numbers dialed. *Miller*, 425 U.S. at 440 (bank records); *Smith*, 442 U.S. at 742 (telephone numbers). However, the Supreme Court has recently and repeatedly recognized that new technologies require a different approach. *See Carpenter*, 138 S. Ct. at 2214; *Riley*, 573 U.S. at 393 (comparing a physical search to the search of a cell phone is like "saying a ride on horseback is materially indistinguishable from a flight to the moon"); *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) (the third-party doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks") (Sotomayor, J., concurring). As a result, any extension of old rules to digital data "has to rest on its own bottom." *Riley*, 573 U.S. at 393.

48. In *Carpenter*, the Supreme Court expressly distinguished cell phone location data, holding that "there is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today." *See* 138 S. Ct. at 2219. Moreover, the Court was clear that the doctrine must not be "mechanically" applied in the digital age. *Id.*

49. Because keyword search data is even more private than the location data in *Carpenter*, it is also "qualitatively different" from the telephone numbers and bank records in *Smith* and *Miller*. *See id.* at 2216–17. It is "detailed, encyclopedic, and effortlessly compiled," *id.* at 2216, as well as deeply revealing. Granting the government the ability to search across all of this information is an unprecedented new surveillance power, allowing investigators to go back in time and learn what someone was thinking, all without expending physical resources.

50. Indeed, in her concurrence in *Jones*, Justice Sotomayor anticipated constitutional concerns regarding searches of keyword data. She insisted that the Fourth Amendment must evolve with changing technological realities and expressed her "doubt that people would accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year." 565 U.S. at 418 (Sotomayor, J. concurring); *see also United States v. Moalin*, 973 F.3d 977, 993 (9th Cir. 2020) (expressing doubt that warrantless collection of metadata comported with the Fourth Amendment, citing Justice Sotomayor's concurrence in *Jones*).

51. The fact that people convey their search queries to Google does not lessen their privacy interest in their search history. In this sense, using a search engine to run keyword searches is like using a cell phone to make cell phone calls—it necessarily involves a third-party service provider. As the *Carpenter* Court explained, "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data." 138 S. Ct. at 2220. The same holds true for search queries. There is no way to run a search query without conveying that information to the search engine. Moreover, using a search engine, like using a cell phone, is "such a pervasive and insistent part of daily life" that it is "indispensable to participation in modern society." *Id.* (citations omitted). Like consulting the card catalogue in a library, it is the way people find what they are looking for online. It is often the first place people turn for whatever information they need, the gateway to the internet. Consequently, "in no meaningful sense does the user voluntarily 'assume the risk'" of turning over a comprehensive dossier of his search activity to law enforcement. *Id.* (citation omitted).

52. Critically, Google logs search queries for everyone who runs a Google search, regardless of whether they are logged in to a Google account. If a user is logged-in to a Google account at the time of the search, Google pairs that search with the account using a GAIA ID. If a user is not logged-in, Google still records and stores their searches. In that instance, however, the information is paired to a Browser Cookie ID rather than a GAIA ID. Furthermore, users who are not logged-in have no ability to delete this data once it has been collected. *See* Google, *Search History*, https://perma.cc/7XKJ-XWUN (last visited June 29, 2022) (showing users preference options for non-registered Google Search users and providing no option to prevent data collection or control data use once it has been collected).

53. Consequently, a keyword warrant "runs against everyone," *Carpenter*, 138 S. Ct. at 2218, because there is no way for users to prevent their keyword searches from being captured by Google. Indeed, the warrant here returned three queries that were not paired with a GAIA ID, only a Browser Cookie ID, indicating that those users were not logged-in to a Google account. In short, users like Mr. Seymour do not "voluntarily" record this information in any meaningful way; there is no choice with Google.

54. Finally, Google's Terms of Service and Privacy Policy have little if any bearing on Fourth Amendment expectations of privacy. *See, e.g., United States v. Irving*, 347 F. Supp. 3d 615, 621 (D. Kan. 2018) (rejecting government's argument that defendant had no expectation of privacy in his Facebook account information where he agreed to Facebook's terms that "generally inform[ed] users that Facebook collects a user's content and information."). Although cell phone users sign contracts with cell phone services providers, the Supreme Court has never allowed such agreements to determine the contours of the Fourth

Amendment. *See Smith*, 442 U.S. at 745 ("We are not inclined to make a crazy quilt of the Fourth Amendment"). Indeed, the *Carpenter* majority never mentioned Mr. Carpenter's contract or terms of service. Instead, the Court looked to the realities of the relationship between cell phone users and cell phone companies, and it determined that people do not "voluntarily" convey sensitive data to the cell phone service provider in any "meaningful sense." 138 S. Ct. at 2220. If anything, Google's Privacy Policy indicates that search history data is private data owned by the account holder, not a Google business record. *See* Attachment 9 (Google Privacy Policy) ("When you're signed in, we also collect information that we store with your Google Account, which we treat as personal information."). Additionally, it is critical to note that Mr. Seymour was just a child—twelve years old—when he created his Google account on September 6, 2016. Google's own terms require individuals to be at least 13 years old to create an account, undercutting any argument that he provided voluntary and meaningful consent to a search of his account. Google, *Age Requirements on Google Accounts*, https://perma.cc/Z6XG-N795 (last visited June 30, 2022).

55. The Supreme Court has never sanctioned a warrantless search of Google data, let alone a search of billions of people's data. On the contrary, a reverse keyword search is precisely the kind of "permeating police surveillance" that the Court has repeatedly warned against. *Di Re*, 332 U.S. at 595 (accord. *Carpenter*, 138 S. Ct. at 2214). Only the vanishing few who can move through life without Google searches "could escape this tireless and absolute surveillance." *Carpenter*, 138 S. Ct. at 2218. This court should therefore conclude that the third-party doctrine does not apply to Google search data.

C. This is a search because users have a possessory interest in their keyword search data.

56. Government conduct is a Fourth Amendment search if it involves an incursion into areas where someone has a property interest. Mr. Seymour, as well as the billions of others whose information was collected in this reverse search, has a property interest in his Google search history. And because the government infringed upon this interest, it was a search under a "property-based" interpretation of the Fourth Amendment. *See Carpenter*, 138 S. Ct. at 2257 (Gorsuch, J., dissenting).

57. Terms of service have little relevance in a *Katz*-type analysis, where the question is what society, not Google, is prepared to accept as reasonable. But a more "traditional approach" asks "if a house, paper or effect was *yours* under law." *Id.* at 2267–68. If it was, "[n]o more [is] needed to trigger the Fourth Amendment." *Id.* This understanding of the Fourth Amendment predates *Katz* and has been repeatedly identified by the Supreme Court as an equally valid and independent test for determining whether a search occurred. *See*, *e.g.*, *Jones*, 565 U.S. at 409; *Kyllo*, 533 U.S. at 37; *Soldal v. Cook County*, 506 U.S. 56, 62 (1992) ("our cases unmistakably hold that the Amendment protects property as well as privacy").

58. Thus, it is highly relevant to a property-based analysis that Google treats search history as personal data that belongs to the user who created it. As Google explains to users, "Your content remains yours, which means that you retain any intellectual property rights that you have in your content." *See* Attachment 26 (Google Terms of Service) at 4. Justice Gorsuch quoted this language—word for word—in *Carpenter* as an example of the type of positive law

that would likely establish a property right in one's digital "papers." 138 S.Ct. at 2242 (Gorsuch, J., dissenting).

59. Google's licensing provisions also reinforce the existence of an individual property right. When creating an account, users agree to provide Google with a license to use any content they create if it is protected by intellectual property rights. Google, *Terms of Service*, https://perma.cc/N4QE-MPLA (last visited Apr. 15, 2022). The license gives Google the right to analyze user content to provide "recommendations and personalized search results, content, and ads." *Id*. And it indicates that the words someone types into the Google search box belong to the user, not to Google. Google simply has permission to use that information according to the license agreement. There are seemingly infinite combinations of letters, words, and phrases that any person can put together when searching for something online, and according to Google's terms of service, people have a property interest in whatever queries they create.

60. Attendant to this property interest, Google recognizes that its users "expect Google to keep their information safe, even in the event of their death," allowing a user to specify who can have access to their records after death, or in the alternative whether Google should delete the data. *See* Google, *Submit a Request Regarding a Deceased User's Account*, https://perma.cc/SY7D-LK95 (last visited Apr. 15, 2022). Account holders are also able to download their data and request that Google delete it at any time using the Google Takeout service, however Google Takeout does not give users the option to wholly opt out of data collection. *See* Google, *How to Download Your Google Data*, https://perma.cc/TGZ3-LVAM (last visited Apr. 15, 2022). The Google Takeout webpage can only be accessed by users with a registered Google account.

61. The fact that Google fulfills requests from government agencies in response to valid warrants does not undermine anyone's property interest in the underlying data. On the contrary, the fact that the government sought a warrant and now seeks to defend its legality is evidence that a Fourth Amendment search occurred. *See Chatrie*, 2022 WL 628905, at *20 n.34 (assuming that the government's collection of geofence location data was a "search" because police sought a warrant); *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 736 (N.D. Ill. 2020) (noting that by obtaining a warrant and arguing for the validity of that warrant, "the government is treating its proposed capture of information as a search"). Moreover, Google's policies set forth discrete circumstances where it will disclose information to law enforcement; all of them imply that law enforcement has identified a known target. They do not suggest that law enforcement will be permitted to conduct fishing expeditions, nor do they inform users of such a possibility.

62. On the contrary, Google represents that information like search history is private user data that cannot be publicly disclosed. It is not Google's data; it is the users' data, which Google holds in trust. Consequently, Google users can exclude others from their account data, which is "one of the most treasured strands" of the property rights bundle. *Loretto v. Teleprompter Manhattan CATV Corp*., 458 U.S. 419, 435 (1982) ("The power to exclude has traditionally been considered one of the most treasured strands in an owner's bundle of property rights."); *see also Kaiser Aetna v. United States*, 444 U.S. 164, 176 (1979) (called the right to exclude "one of the most essential sticks" in the in the "bundle of rights that are commonly characterized as property-the right to exclude others"); William Blackstone, 2 Commentaries

on the Laws of England, at *2 (1771) (defining property as "that sole and despotic dominion … exercise[d] over the external things of the world, in total exclusion of the right of any other ….").

63. The Supreme Court recently recognized that individuals have a Fourth Amendment interest in rental cars owned by a third-party company, just as guests have a privacy interest in their rented hotel rooms. *See Byrd v. United States*, 138 S. Ct. 1518, 1528 (2018) (There is "no reason why the expectation of privacy that comes from lawful possession and control and the attendant right to exclude would differ depending on whether the car in question is rented or privately owned…much as it did not seem to matter whether the friend of the defendant in *Jones* owned or leased the apartment he permitted the defendant to use in his absence."). Indeed, if someone else stole Mr. Seymour's search records from Google, he could recover damages in a traditional tort action. *Cf. Carpenter*, 138 S. Ct. at 2242 (Gorsuch, J., dissenting). Similarly, anyone who accesses Mr. Seymour's Google account without authorization could be held criminally liable under the Stored Communications Act ("SCA"). *See* 18 U.S.C. § 2701(a). Here, Google structured its services to reflect the SCA's mandate, giving users the ability to exclude anyone from accessing their information. As a result, users like Mr. Seymour have a property interest in their Google search history data.

64. When law enforcement searched and seized Mr. Seymour's Google data, it eliminated his ability to exclude others from it. This intrusion violated Mr. Seymour's possessory interest in his data, therefore indicating that a Fourth Amendment search occurred.

* * *

65. People have both a reasonable expectation of privacy and a possessory interest in their keyword search data. Consequently, law enforcement's acquisition of that data was a Fourth Amendment search. Furthermore, the third-party doctrine does not apply because Mr. Seymour did not voluntarily convey his keyword search data to Google.

II. The keyword warrant is unconstitutional.

66. The Fourth Amendment requires that a warrant (1) be supported by probable cause; (2) particularly describe the place to be searched and the things to be seized; and (3) be issued by a neutral disinterested magistrate. *Dalia v. United States*, 441 U.S. 238, 255 (1979). When Fourth Amendment searches implicate First Amendment concerns, courts must be careful to apply the Fourth Amendment's requirements with "the most scrupulous exactitude," mindful that "leaving the protection of [First Amendment] freedoms to the whim of the officers charged with executing the warrant" is unconstitutional. *Stanford*, 379 U.S. at 485; *see also Tattered Cover*, 44 P.3d at 1047.

67. The keyword warrant in this case is a prime example of an indiscriminate, "dragnet type law enforcement practice[]," sweeping up the search history data of billions in the hopes of finding one potential lead. *United States v. Knotts*, 460 U.S. 276, 284 (1983). It is a general warrant, an overbroad request that fails to meet the requirements of probable cause and particularity. It is antithetical to the Fourth Amendment. It is not even close to satisfying the Fourth Amendment requirements with "scrupulous exactitude," despite the inherent First Amendment

concerns involved. *Stanford*, 379 U.S. at 485. Due to these constitutional deficiencies, the warrant is unconstitutional under the Fourth Amendment and its fruits should be suppressed.

A. The keyword warrant is a prohibited general warrant.

68. Keyword warrants pose the same threats that general warrants and writs of assistance posed at the time of the Founding. General warrants "allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity," and were one of the direct causes that led to American revolution. *Riley*, 573 U.S. at 403. General warrants were despised because they "specified only an offense…and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." *Steagald v. United States*, 451 U.S. 204, 220 (1981). The same is true of the keyword warrant here. Keyword warrants intrude on the privacy of protected spaces like the home, generating fear that anyone might become the subject government scrutiny in their most private spaces. *See Silverman v. United States*, 365 U.S. 505, 511 (1961) ("At the very core [of the Fourth Amendment] stands the right of a [person] to retreat into his own home and there be free from unreasonable governmental intrusion.").

69. The prohibition of general warrants remains a central tenet of American ideals, given that opposition to general warrants "helped spark the Revolution itself." *Carpenter*, 138 S. Ct. at 2213; *see also Riley*, 573 U.S. at 403; *Stanford*, 379 U.S. at 481; *Marcus v. Search Warrant of Property*, 367 U.S. 717, 728 (1961). In fact, general warrants are key to understanding why the Fourth Amendment exists. *See Stanford*, 379 U.S. at 482–83 (describing the "battle for individual liberty and privacy" as won when British courts stopped the "roving commissions" given authority "to search where they pleased"). General warrants did not specify which houses to search or whom to arrest; instead, "discretionary power [was] given to messengers to search wherever their suspicions may chance to fall," leading to the destruction of property and the arrest of dozens of people. *Wilkes v. Wood*, 98 Eng. Rep. 489, 498 (1763). General warrants left "the liberty of every man in the hands of every petty officer" and were ultimately denounced as "the worst instrument of arbitrary power." *Stanford*, 379 U.S. at 481 (citation omitted).

70. The prohibition on general warrants restricts the government from exercising "arbitrary power." *Id.* And by requiring sufficient probable cause and particularity, the Fourth Amendment limits both the scope of searches and the discretionary power of law enforcement. *See* Laura K. Donohue, *The Original Fourth Amendment*, 83 U. Chi. L. Rev. 1181, 1298–1305 (2016) (describing the drafting process of the Fourth Amendment). For example, a warrant to search every house in the neighborhood or every person at a bar would be plainly unconstitutional. It is axiomatic that probable cause must be based on individualized facts, not group probabilities. *See Ybarra v. Illinois*, 444 U.S. 85, 91 (1979); *United States v. Curry*, No. 3:17-CR-130, 2018 WL 1384298, at *11 (E.D. Va. Mar. 19, 2018) ("[G]eneralized suspicion and fear cannot substitute for specific and articulable facts") (citations and quotation marks omitted), *aff'd*, 965 F.3d 313 (4th Cir. 2020); *United States v. Glenn*, No. CR-609-027, 2009 WL 2390353, at *5 (S.D. Ga. 2009) (A "generalized belief that some of the patrons whom [police] had targeted for a systematic patdown might possibly have a weapon was insufficient to justify a cursory frisk of everyone present." (quotation marks omitted)); *Commonwealth v. Brown*, 861 N.E.2d 504, 505 (Mass. App. Ct. 2007) (finding a warrant "authorizing a search

of 'any person present'…. resulted in an unlawful general search"); *Carroll v. United States*, 267 U.S. 132, 153–54 (1925) (stating it would be "intolerable and unreasonable" to "subject all persons lawfully using the highways to the inconvenience and indignity" to a search just because some cars may contain contraband); *Grumon v. Raymond*, 1 Conn. 40, 43 (1814) (holding a "warrant to search all suspected places" for stolen goods was unlawful because "every citizen of the United States within the jurisdiction of the justice to try for theft, was liable to be arrested"). But, with a keyword warrant like the one, the government defies this fundamental instruction and predicates probable cause on group probabilities. If such a warrant is deemed valid, the government can search more than a home or pockets; it can search through users' thoughts as expressed in searches, without probable cause or particularized suspicion as to any one individual person.

71. Keyword warrants represent precisely the sort of undirected, unrestrained search of constitutionally protected areas as the reviled general warrants of old. And when deciding if a search is constitutional, the Supreme Court has always been "careful to distinguish between [] rudimentary tracking…and more sweeping modes of surveillance." *Carpenter*, 138 S. Ct. at 2215 (citing *Knotts*, 460 U.S. at 284). Reverse keyword warrants are nothing if not "sweeping," and therefore fall in the most concerning category of searches. In *Knotts*, the Supreme Court cautioned against this exact kind of surveillance, noting that "if such dragnet type law enforcement practices … should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." 460 U.S. at 283–84. That time is now.

72. Law enforcement did not—and could not—identify beforehand whose Google data they planned to search and seize. Consequently, the government failed to establish probable cause as to any one of the billions of Google users whose data it searched. *See Chatrie*, 2022 WL 628905, at *18 (finding that the warrant violates the Fourth Amendment because the government "[l]acked [p]articularized [p]robable [c]ause as to [e]very Google [u]ser in the [g]eofence). As discussed below, this keyword warrant cannot meet the probable cause and particularity requirements of the Fourth Amendment and is therefore an invalid general warrant.

B. The keyword warrant lacks probable cause to justify such an overbroad search.

73. The keyword warrant in this case involved a search of every single Google query over the course of 15 days. It was a modern-day digital dragnet, conducted by the world's largest search engine company, at the government's direction. The government commandeered Google to search through nearly a billion private accounts, in addition to the billions of other searches conducted by users who were not logged in.[8] If the government had probable cause to search

[8] Google does not report daily search statistics, but in 2016 the company reported that it processes "trillions" of searches per year. Danny Sullivan, *Google Now Handles At Least 2 Trillion Searches Per Year*, Search Engine Land (May 24, 2016), https://perma.cc/5KXC-JC7G. It is safe to assume that the search engine meant that it processes at least two trillion searches per

one account, it would have done so. It did not. Instead, it searched billions to determine if any of them contained data of interest. The warrant is the very definition of overbroad, and this court should find it unconstitutional.

74. The Supreme Court has been clear that the scope of a search must be tailored to the probable cause in each case. Probable cause is "a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). And a warrant must be "no broader than the probable cause on which it is based." *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006) (quoting *United States v. Zimmerman*, 277 F.3d 426, 432 (3d Cir. 2002)). Law enforcement must have "a reasonable ground for belief of guilt…particularized with respect to the person to be searched or seized." *Maryland v. Pringle*, 540 U.S. 366, 371 (2003) (citations and quotation marks omitted). Particularized probable cause "cannot be undercut or avoided by simply pointing to the fact that coincidentally there exists probable cause to search or seize another or to search the premises where the person may happen to be." *Ybarra*, 444 U.S. at 91. Rather, there must be a logical "nexus" between the crime and the evidence to be seized, *see* LaFave, 2 Search and Seizure § 3.7(d) (6th ed. 2021), not assumptions about what a suspect might have searched for.

75. Here, the government did not have probable cause to search even one account. The statement of probable cause was nearly identical to the statements used for the first two failed keyword warrants. *Compare* Attachment 1 (Nov. 19 Keyword Warrant) at 3053–59 *with* Attachment 2 (Oct. 1 Keyword Warrant) at 2596–601 and Attachment 3 (Oct. 20 Keyword Warrant) at 3063–68. All of them relied on the same description of surveillance video obtained from a neighboring home, showing three suspects in a yard. Attachment 1 (Nov. 19 Keyword Warrant) at 3055–56. But nothing in that description mentioned a cell phone or Google. It did not state that the suspects were seen holding a phone. It did not state that the suspects were seen using one. Instead, it cited the "personal nature of this offense" and "the amount of planning that likely went into a coordinated attack such as this one," as well as the fact that the house was not on a corner lot. *See id.* at 3058. Based on nothing more, it concluded that there was a "reasonable probability that one or more of the suspects searched for directions to the victim's address prior to the fire." *Id*.

76. This was pure, unsupported conjecture. At the time, investigators simply "didn't know" who they were looking for. Prelim. Tr. at 84. They thought it might have been someone living in the house. *See id.* at 83. They thought it might have been someone with a personal vendetta against the family. *Id.* at 64–65. They thought it might have been a random person. *Id.* at 84–85. They simply did not know if, whether, or why someone may have searched Google for

---

year, which would put average daily Google searches at around 5.5 billion. Given that the volume of Google searches increases substantially year to year, it is likely that the number is significantly higher. *See, e.g.,* Kris Reid, *How Many Google Searches Per Day On Average In 2022?,* Ardor SEO (2022), https://perma.cc/78HE-HNNK. Internet Live Stats reports that there are approximately 100,000 Google search queries every second, which would translate to over 8 billion searches per day. *Google Searches in 1 Second*, Internet Live Stats, https://perma.cc/CG3G-RN67.

5312 Truckee Street. *Id.* at 84 ("we did not know at all why this had occurred"). In short, investigators lacked probable cause to search any one individual's search history, so instead relied on speculation and generalized suspicion to search billions.

77. The government's justification for the keyword warrant is backwards, and it has been recently rejected in analogous geofence cases. For example, a federal court in Illinois rejected a geofence warrant application, finding that the government's position "resembles an argument that probable cause exists because those users were found in the place…[where] the offense happened," an argument the Supreme Court rejected in *Ybarra*. *See In re Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 751. The court further stated:

> [I]f the government can identify that wrongdoer only by sifting through the identities of unknown innocent persons without probable cause and in a manner that allows officials to rummage where they please in order to see what turns up, even if they have reason to believe something will turn up, a federal court in the United States of America should not permit the intrusion. Nowhere in Fourth Amendment jurisprudence has the end been held to justify unconstitutional means.

Id. at 754 (citations and quotation marks omitted). More recently in *Chatrie*, the court found "unpersuasive the United States' inverted probable cause argument—that law enforcement may seek information based on probable cause that some unknown person committed an offense, and therefore search every person present nearby." *Chatrie*, 2022 WL 628905, at *24. That inverted probable cause argument is the same one being made regarding keyword warrants in this case and similarly must be rejected.

78. In sum, the keyword warrant here is void for overbreadth. It authorized an unconstitutional search that lacked any individualized suspicion. Indeed, there is no amount of probable cause that could justify a search of such magnitude. Here, law enforcement did not indicate probable cause for even a single Google user caught up in the keyword dragnet. The keyword warrant was therefore unconstitutional for lack of probable cause.

C. The keyword warrant lacks particularity.

79. The Fourth Amendment requires that warrants "particularly describ[e]…the…things to be seized." U.S. Const. amend. IV. A warrant's description of "what is to be taken" must leave "nothing…to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927); *see also Stanford*, 379 U.S. at 481. The particularity requirement demands that a warrant spell out precisely what is within its scope because law enforcement officers are prohibited from "seizure of one thing under a warrant describing another." *Marron*, 275 U.S. at 196. A valid warrant must confine "the executing [officers'] discretion by allowing them to seize only evidence of a particular crime." *United States v. Cobb*, 970 F.3d 319, 332 (4th Cir. 2020) (quoting *United States v. Fawole*, 785 F.2d 1141, 1144 (4th Cir. 1986), *as amended* (Aug. 17, 2020), *cert denied*, 141 S. Ct. 1750 (2021). A valid warrant limits searches and seizures exclusively to evidence that is related to a specific crime. *See Andresen v. Maryland*, 427 U.S. 463, 481–83 (1976). Consequently, it is impermissible to search through a person's data when that person has nothing to do with the crime in question. The keyword warrant here violates the particularity requirement by granting the government and Google

broad discretion to search private data, neglecting the fact that the vast majority of the data searched was inevitably unrelated to the criminal investigation.

80. The warrant did not establish probable cause that is "particularized with respect to the person to be searched or seized." *Pringle*, 540 U.S. at 371. Instead, it operated in reverse, requiring Google to search and produce data for *all* users who searched for one of nine variations of an address over the course of 15 days. This reverse search process is like the geofence warrant in *Chatrie*, which was found unconstitutional for lack of particularity because it captured data from people who were not even suspected to be involved with the crime. 2022 WL 628905, at *14. That search swept up people who were nowhere near the incident, including people at home in a nearby apartment complex, dining at a Ruby Tuesday restaurant, and driving next to a nearby church. *Id.*. Similarly, here, the keyword warrant encompasses people who may have searched for a local address, with no restrictions to filter out people who searched specific terms for reasons unconnected to the crime under investigation.

81. Additionally, the warrant is not particularized because it does not adequately describe the data to be searched. While it identified an address for Google headquarters, "1600 Amphitheater Parkway," it did not identify any accounts to be searched there. Instead, it gave law enforcement the discretion to rummage through everyone's keyword data. By contrast, in *People v. Coke*, the Colorado Supreme Court held that a warrant authorizing a search of a single suspect's cell phone lacked particularity because it permitted law enforcement to search the device for any incriminating information. 461 P.3d 508, 516 (Colo. 2020). If an unconstrained search of a single, previously identified suspect's information lacks particularity, then an unconstrained search of a *billion unidentified* users' information is infinitely more egregious.

82. At the very least, the government should be required to identify the target Google accounts to search through "objective guardrails" and benchmarks. *Chatrie*, 2022 WL 628905, at *25 But that is not what happened here. The warrant made no attempt to limit the number of accounts subject to search. And the error was only compounded by requiring the disclosure of identifying IP addresses. As discussed in part III(C), *infra*, including IP addresses in the initial warrant return rendered the "de-identification" procedure meaningless and misleading.

83. The particularity requirement is at its most stringent when the items to be searched and seized raise First Amendment concerns. *Stanford*, 379 U.S. at 485. That is because some searches, as with the keyword warrant here, have the potential to burden bystanders' freedom of inquiry and association. Indeed, disclosing associations to the government "can chill association 'even if there is no disclosure to the general public.'" *Ams. for Prosperity Found. V. Bonta*, 141 S. Ct. 2372, 2388 (quoting *Shelton v. Tucker*, 364 U.S. 479, 486 (1960)). Likewise, disclosing search queries is as close to mind-reading as the government can get. For most Americans, the Google search box is a place of curiosity, convenience, and even confession. We ask of the machine what we do not dare dream to ask of other people. Google searches are often one of the most private things we do. They reveal not just our activities, but our intentions, our goals, and our deepest fears.

84. In this instance, the search would have swept up anyone looking for directions to a friend's house or hoping to learn about a colleague. The warrant was not narrow; it required Google to

search *everyone*. And it is not a stretch to imagine similar warrants seeking data about a controversial political event or a local women's health clinic. The Fourth Amendment is especially important for these reasons, and the warrant here failed to meet the heightened threshold for warrants that raise First Amendment concerns. It was a digital general warrant, lacking both probable cause and particularity, and this Court should find it unconstitutional.

III. The good-faith exception does not apply.

85. Under Colorado law, the good-faith exception is limited to when law enforcement acts "as a result of a good-faith mistake or a technical violation." Colo. Rev. Stat. Ann. § 19-2.5-906. This test is substantially similar to the "objectively reasonable" standard articulated by the U.S. Supreme Court in *United States v. Leon*, 468 U.S. 897, 926 (1984), but with a presumption that an officer was acting in good faith if acting pursuant to a warrant. *People v. Randolph*, 4 P.3d 477, 483 (Colo. 2000). Nonetheless, suppression is appropriate and the good-faith exception does not apply if the officer "failed to undertake the search in a good-faith belief that it was reasonable." *Id.*; *see also Leon*, 468 U.S. at 926. As in *Leon*, the good faith exception does not apply in at least four circumstances: (1) where a warrant is based on knowing or recklessly false statements, *Leon*, 468 U.S. at 914 (citing *Franks v. Delaware*, 438 U.S. 154 (1978)); (2) where the judge acted as a rubber stamp for the police, *id.* (citing *Gates*, 462 U.S. at 239); (3) where a warrant affidavit lacks a substantial basis to determine probable cause*, id.* at 915 (citing *Gates*, 462 U.S. at 239); and (4) where no officer could reasonably presume the warrant was valid*. Leon*, 468 U.S. at 926.

86. Here, the good faith exception does not apply because of (1), (3), and (4). The warrant affidavit misled the court as to the breadth of the search, the lack of statutory authorization, and the so-called "de-identified" nature of the data. And it was so lacking in probable cause and particularity that no officer could reasonably presume it was valid. Instead, it was invalid from the beginning. *See Groh v. Ramirez*, 540 U.S. 551, 558 (2004) (finding a warrant "so obviously deficient" in particularity that "we must regard the search as 'warrantless' within the meaning of our case law.").

A. Knowing or Recklessly False Statements

87. Investigators were anxious to solve this case. They obtained search warrants for specific individuals' cell phone and Google data. Prelim. Tr. at 72-76. But when these efforts proved unfruitful, their tactics shifted. Prelim. Tr. at 47. They cast digital dragnets, each bigger than the last, without identifying any suspects at all. Investigators issued "very general" search warrants, *id.* at 61–62, sweeping up hundreds and thousands of people with two tower dumps and an IMSI catcher, and then hundreds of millions of people with the geofence and Fog Data warrants. Prelim. Tr. at 70–71, 127–28. It was a parade of general warrants, demonstrating investigators' repeated willingness to violate the privacy rights of Coloradans *en masse*. *See supra*, ¶¶ 8–13. And the keyword warrant was the biggest dragnet of them all.

88. Det. Sandoval submitted the keyword warrant application, and when he did, he was aware, or should have been aware, that it would entail the search of billions of people. Yet the application failed to disclose this critical fact to the issuing judge. It failed to convey that it was seeking to use a novel type of "reverse" warrant to search *everyone*, without limitation, who conducted a

Google search over the course of 15 days. And this lack of candor was highly consequential. *See People v. Winden*, 689 P.2d 578, 583 (Colo. 1984) (recognizing that an application "may be so misleading because of the omission of material facts known to the affiant at the time the affidavit was executed that a finding of probable cause based on such statements may be deemed erroneous").

89. Had Det. Sandoval said that police planned to conduct a search of billions, no judge in the country would have signed the warrant. Such language would have immediately revealed the complete lack of probable cause to cast such an indiscriminately broad net. But Det. Sandoval omitted the most critical facts with a reckless disregard for the truth, concealing the true scope of the search, and substantially misleading the judge. *See id.; People v. Kerst*, 181 P.3d 1167, 1171 (Colo. 2008); *see also Groh,* 540 U.S. at 561 n.4 (where government agent did not alert the magistrate to the defect in the warrant that the agent had drafted, the Court could not be certain whether the magistrate was aware of the scope of the search he was authorizing); *see also United States v. Rettig*, 589 F.2d 418, 422 (9th Cir. 1978) ("By failing to advise the judge of all the material facts, including the purpose of the search and its intended scope, the officers deprived him of the opportunity to exercise meaningful supervision over their conduct and to define the proper limits of the warrant.").

90. Furthermore, had Det. Sandoval truthfully described the nature of the keyword warrant, it would have been clear that the Stored Communications Act does not authorize such reverse searches. The affidavit relies on the SCA, 18 U.S.C. § 2703, as a basis for the warrant. *See* Attachment 1 (Nov. 19 Keyword Warrant) at 3052. The SCA, however, requires that police identify particular people to search. It limits the government to obtaining a warrant for records pertaining to "a subscriber to or customer of" the provider. 18 U.S.C. § 2703(c)(1). This authorization is phrased in the singular and does not contemplate, let alone permit, astronomically large searches of unidentified people. Furthermore, the SCA prohibits the government from obtaining records that are not "relevant and material" to the ongoing criminal investigation. *See* 18 U.S.C. § 2703(d). Yet, by dint of operation, nearly all of the records searched and seized with a keyword warrant have no connection to the crime under investigation.[9]

[9] At minimum, the "relevant and material" requirement under the SCA is more demanding than the mere "relevance" standard governing the issuance of administrative and grand-jury subpoenas. *See In re Application of U.S. for an Order for Disclosure of Telecomms. Records & Authorizing the Use of a Pen Register and Trap and Trace*, 405 F. Supp. 2d 435, 448 (S.D.N.Y. 2005) (Gorenstein, M.J.); *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 752 (S.D. Tex. 2005) (Smith, M.J.). Under the lower "relevance" standard, courts have consistently required that the particular records demanded by the government have an actual connection to a particular investigation. *See, e.g.*, *Bowman Dairy Co. v. United States*, 341 U.S. 214, 221 (1951) (invalidating a subpoena's "catch-all provision" on the grounds that it was "merely a fishing expedition to see what may turn up"). Courts have also rejected or narrowed subpoenas that, because they fail to identify the outer bounds of the categories of records they seek, cover large volumes of *irrelevant* documents. *See In re Grand Jury Subpoena*

91. Where, as here, the government indiscriminately seeks records implicating the privacy of hundreds or thousands of individuals in one fell swoop, it cannot possibly meet the SCA's "relevant and material" standard, let alone the probable cause standard, needed to search *all* Google search users. *See Chatrie*, 2022 WL 628905, at *18 (finding that a geofence warrant "[l]acked [p]articularized [p]robable [c]ause as to [e]very Google [u]ser" searched). Any reliance on the SCA was thus objectively unreasonable. *See Illinois v. Krull*, 480 U.S. 340, 360 n.17 (1987) (declining to apply good faith exception "when police officers act outside the scope of a statute, albeit in good faith"). A reverse keyword warrant is plainly not the kind of search authorized by the SCA and citing it here was reckless and misleading.

92. It is possible that Det. Sandoval did not know exactly how many people would be searched by the keyword warrant, but this is no excuse. He signed the affidavit and then executed the warrant. Thus, "[a]t each stage, he had a duty to exercise his independent good judgment to assure himself that the affidavit was sufficient." *Randolph*, 4 P.3d at 484. It is not acting in "good faith" to obtain a warrant for a search that the affiant does not understand and fails to explain to the issuing judge. *See Franks*, 438 U.S. at 163 n.6 (recognizing that police cannot "insulate one officer's deliberate misstatement merely by relaying it through an officer-affiant personally ignorant of its falsity").

93. It is apparent, however, that investigators had at least some idea of the scope of the search. Det. Baker stated, albeit mistakenly, that he believed the search covered the entire state of Colorado. *See* Prelim. Tr. at 81–82 ("I believe we limited it to Colorado for that search – that keyword search on that warrant."); *see also id.* at 132 (recognizing that "Google is in the data collection business" and that "if you are logged into a Google account and are doing things with your Google products, they will be able to attribute whatever it is that you're doing back to your account."). The affidavit, however, does not mention searching everyone in Colorado, let alone the warrant's true scope: everyone in the world who searched Google.

94. Finally, the application omitted that Google had refused to comply with two previous keyword warrants that were signed by a different judge. Google did not comply with the October 1, 2020, warrant because it violated their policy regarding "de-identification of responsive productions" by seeking full names and addresses for all responsive queries. *See* Exhibit 4 (Declaration of Nikki Adeli) ¶ 11. Likewise, Google did not comply with the October 20, 2020, warrant because it sought detailed user location data in addition to "anonymized" results. *See id.* ¶ 13. But Det. Sandoval failed to provide any of this information to Judge Zobel in the November 19, 2020, warrant application. Had the court been informed of these previous doomed attempts, it would have been apparent that requiring the production of identifying information, including IP addresses, defeats the so-called "de-identification" procedure outlined in the second and third warrants.

95. By requiring Google to provide full IP addresses for every responsive query, investigators knew that they would be able to link individual queries to particular people, regardless of whether Google tried to anonymize the results by using "truncated" GAIA or Cookie IDs.

Duces Tecum *Dated Nov. 15, 1993*, 846 F. Supp. 11, 12 (S.D.N.Y. 1994) (quashing a grand-jury subpoena that demanded the entire contents of "computer hard drives and floppy disks," because the materials "contain[ed] some data concededly irrelevant to the grand jury inquiry").

Investigators knew this because they said so in the December 4, 2020, warrant application seeking subscriber information from internet service providers based on the responsive IP addresses. *See* Attachment 17 (Google Search Warrant) at 2606 ("In addition, email providers often have records of the Internet Protocol address ('IP address') used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account."). Indeed, that is how investigators identified Mr. Seymour as a suspect in this case. But Det. Sandoval made no mention of this fact, or of the previous two warrants, in his November 19 application. Had he done so, it would have been apparent that that the "de-identification" procedure described was a farce. Instead, the omission substantially misled the court once again.

96. In sum, the government failed to apprise the judge of critical facts that prevented him from exercising his constitutional function of ensuring that warrants are valid. The government failed to state that the warrant would search billions of people, and at least everyone in Colorado. In so doing, the government also misled the court about the (in)applicability of the Stored Communications Act. And the government failed to note its previous attempts to serve keyword warrants on Google and the reasons Google refused to comply. Had these facts been presented to the judge, it would have been clear that this warrant authorized the search of billions of people, without the promised "de-identification" process. These facts would have revealed the true nature and scope of the keyword warrant, as well as the truth that the police did not—and could not—have probable cause to justify a reverse search of global scale.

B. Lacking in Indicia of Probable Cause

97. Additionally, the good-faith exception does not apply because the keyword warrant was "so lacking in indicia of probable cause" to search Mr. Seymour that it was entirely unreasonable for an officer to rely on it. *See Leon*, 468 U.S. at 923 (citations and quotation marks omitted). The warrant, truthfully understood, authorized the search of billions of Google Search users. But the affidavit did not, and indeed could not, have established probable cause to search so many people at once.

98. The application lacked sufficient "indicia of probable cause" to suggest that evidence of this crime would be found with Google. *See United States v. Gonzales*, 399 F.3d 1225, 1229 (10th Cir. 2005) (rejecting the good-faith exception where law enforcement failed to establish *any* "factual basis connecting the place to be searched to the defendant or suspected criminal activity") (quoting *Leon*, 468 U.S. at 916); *see also People v. Leftwich*, 869 P.2d 1260, 1270 (Colo. 1994) (rejecting the good-faith exceptions where affidavit "contain[ed] no facts that would allow a reasonable officer to conclude that probable cause existed"). Instead, it was based on pure conjecture. The government simply assumed that a cell phone was involved, and that Google had relevant data, despite the fact that two tower dumps, an IMSI catcher, a data broker warrant, and two Google geofence warrants had all failed to produce any leads. The same logic could be invoked in any case, even if, as here, there are no facts to justify it.

99. The only way to describe the keyword warrant here is a dragnet. It was devoid of any individualized suspicion, and there was nothing to indicate a cell phone or computer was involved. Det. Baker later testified that he "felt" the suspects "possibly could have a cellular

phone with them." Prelim. Tr. at 43. But the application did not even mention this feeling, and it did not establish a fair probability that Google would have responsive data. In short, it lacked a substantial basis to determine probable cause for searching anyone's Google data, let alone billions.

100. The so-called "de-identification" process does not change this calculus, because in this case it was meaningless. In addition to "truncated" IDs, the warrant specifically authorized the production of full IP addresses, which the government knew it could use to identify people. And that is exactly what they did to identify Mr. Seymour. *See supra*, ¶¶ 33–36.

101. The government used the same basic statement of probable cause to justify every intrusion in this case, tempered only with vague descriptions of the Orwellian searches they sought to conduct. The keyword warrant was just the last in this long line of digital dragnets, and there was likewise no justification for it, apart from the pressure to solve the case. But even so, obtaining warrants based on conjecture is not "objectively reasonable law enforcement activity." *See Leon*, 468 U.S. at 919. And any reasonable officer would recognize that a dragnet is still a dragnet, no matter how dressed up it might be. The good-faith exception should therefore not apply.

C. Facially Deficient

102. Third, the good faith exception does not apply because the keyword warrant was "facially deficient," and no objective officer could reasonably presume it was valid. *See Leon*, 468 U.S. at 923. A keyword warrant cannot be consistent with the Fourth Amendment because of the broad discretion it gives to police to search and seize data belonging to people with no connection to the crime. It lacks any individualized suspicion and is the digital equivalent of the reviled "general warrants" that gave birth to the Fourth Amendment. *See Carpenter*, 138 S. Ct. at 2213; *see also Riley*, 573 U.S. at 403; *Stanford*, 379 U.S. at 481.

103. Any reasonable officer would have known that such general searches are not only impermissible, but offensive to the most basic principles of American liberty. Indeed, the British use of general warrants was the catalyst for the Fourth Amendment's warrant requirement.[10] The Founders opposed them because of the discretion they gave to officials, placing "the liberty of every man in the hands of every petty officer" and were thus "the worst

[10] One of the specific cases that gave rise to the Fourth Amendment was *Wilkes v. Wood*, which concerned a general warrant that ordered the King's messengers to "apprehend and seize" the printers and publishers of an anonymous pamphlet, the *North Briton* No. 45. The warrant did not specify which houses to search or whom to arrest, but officials ransacked five homes, broke down 20 doors, rummaged through thousands of books and manuscripts, and arrested 49 people. *See* Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 Ind. L.J. 979, 1007 (2011). The *Wilkes* court condemned the warrant because of the "discretionary power" it gave officials to decide where to search and what to take. 98 Eng. Rep. at 498. The case became wildly famous in the American colonies, one of three influential English cases that led to the rejection of general warrants. *See generally*, Donohue, *The Original Fourth Amendment*, 83 U. Chi. L. Rev. 1181. *See also Entick v Carrington*, 19 How St Tr 1029 (CP 1765); *Leach v Money*, 19 How St Tr 1001 (KB 1765).

instrument of arbitrary power." *Stanford*, 379 U.S. at 481 (citations omitted). They allowed the government to target people without any evidence of criminal activity, "turn[ing] the concept of innocent until proven guilty on its head." *See* Donohue, 83 U. Chi. L. Rev. at 1317. Instead of having information that the person or place to be searched is engaged in illegal activity, general warrants presume guilt, establishing innocence only after a search. *Id*. Prohibiting such "promiscuous" searches therefore served to protect not only individual rights, but also establish a cornerstone criminal justice of America. *Id* at 1320.

104. The unique nature of this warrant—a reverse warrant—would have been apparent to investigators. There were no police department policies to follow, no procedures, and no rules about how to conduct a keyword search—because valid warrants do not work this way. The warrant did not direct investigators to seize Mr. Seymour's data or anyone else's; instead, it permitted them to rummage through *everyone's* private Google search history and determine for themselves which to seize. Such "broad authorization" is a "general search" that "violates the particularity demanded by the Fourth Amendment." *Coke*, 461 P.3d at 516; *see also People v. Thompson*, 500 P.3d 1075, 1077 (Colo. 2021) (upholding a trial court's rejection of the good-faith exception because it did not "even come close to the particularity that, in fairness, should have been described").

105. There is no such thing as relying on a general warrant in good faith. *See United States v. Winn*, 79 F. Supp. 3d 904, 926 (S.D. Ill. 2015) ("Because the warrant is a general warrant, it has no valid portions."). Rather, courts have recognized that "[t]he cost to society of sanctioning the use of general warrants—abhorrence for which gave birth to the Fourth Amendment—is intolerable by any measure. No criminal case exists even suggesting the contrary." *United States v. Christine*, 687 F.2d 749, 758 (3d Cir. 1982); *see also United States v. Wecht*, 619 F. Supp. 2d 213, 236–37 (W.D. Pa. 2009); *Coke*, 461 P.3d at 516. Thus, the "the only remedy for a general warrant is to suppress all evidence obtained thereby." *United States v. Yusuf*, 461 F.3d 374, 393 n.19 (3d Cir. 2006). Consequently, this court should find that the good faith doctrine does not apply to the keyword warrant in this case and suppress all evidence and fruits thereof.

REQUEST FOR VERACITY HEARING

106. Both the United States and Colorado Constitutions prohibit the issuance of a search warrant except upon a showing of probable cause supported by oath or affirmation particularly describing the place to be searched and the things to be seized. *People v. Pacheco*, 175 P.3d 91, 94 (Colo. 2006).

107. Probable cause must be established within the four corners of the affidavit in support of the search warrant. *Randolph,* 4 P.3d 477. The affidavit establishes probable cause if the affidavit contains "sufficient facts to warrant a person of reasonable caution to believe that contraband or evidence of criminal activity is located at the place to be searched." *People v. Miller*, 75 P.3d 1108, 1112 (Colo. 2003) (citations omitted).

108. "Our cases have recognized the appropriateness of veracity hearings, which are inquiries into the accuracy of statements found in an affidavit supporting a search warrant, 'at least where

the good faith of the police officer-affiant was explicitly or tacitly at issue.'" *People v. Flores*, 766 P.2d 114, 118 (Colo. 1988) (*citing Dailey*, 639 P.2d 1068, 1073 (Colo. 1982).

109. "[A]s conditions to a veracity hearing testing the truth of averments contained in a warrant affidavit, under our state law we shall require that a motion to suppress (1) be supported by one or more affidavits reflecting a good faith basis for the challenge and (2) contain a specification of the precise statements challenged." *Dailey*, 639 P.2d at 1075. If both parts of this threshold test are met, then "a veracity hearing must be held in order to comply with the Fourth Amendment of the federal constitution." *Winden*, 689 P.2d at 581 (*citing Franks*, 438 U.S. 154).

110. As detailed *supra*, ¶¶ 88–97, and in the attached Affidavit of Michael Juba, *see* Attachment 27, the keyword warrant application failed to disclose critical fact to the issuing judge.

111. The application failed to convey that it was seeking a novel reverse warrant to search billions of people without limitation. It failed to disclose that Google had rejected two previous keyword warrants issued by another judge. And it failed to inform the judge that the IP address information sought would defeat the "de-identification" scheme outlined in the warrant.

112. As a result of these omissions, the application demonstrated a reckless disregard for the truth, concealing the true scope of the search, and substantially misleading the issuing judge. *See Winden*, 689 P.2d at 583; *Kerst*, 181 P.3d at 1171.

113. Mr. Seymour therefore requests a veracity hearing to further establish that the keyword warrant application substantially misled the issuing judge.

CONCLUSION

Keyword warrants represent an unprecedented expansion of the government's surveillance capabilities. *Carpenter*'s emphasis on the degree to which keyword search data obtained by law enforcement is sensitive or "deeply revealing" suggests that courts are recognizing the need to treat keyword search data differently from physical records. Based on the sensitivity of these records and the scope of the search, keyword warrants are Fourth Amendment searches of the unreasonable variety. The warrant obtained in this case implicates First Amendment concerns, and as such must withstand "scrupulous exactitude" under the Fourth Amendment. Yet this warrant cannot even survive the probable cause and particularity requirements under the Fourth Amendment. Instead, it functions as a constitutionally impermissible general warrant. Finally, because the good faith exception cannot apply to a warrant no reasonable law enforcement officer would in good faith rely on, this keyword warrant is an unconstitutional search.

WHEREFORE, Mr. Seymour moves this Court to order a veracity hearing and suppress all evidence obtained from the November 19, 2020, keyword warrant, as well as fruits thereof.

Respectfully submitted,

Date: June 30, 2022

Attorney: Michael W. Price, #22PHV6967

Attorney: Michael S. Juba, #39542

/s/ Jenifer Stinson

Attorney: Jenifer Stinson, #35993

I hereby certify that on this 30th day of June, 2022, a true and correct copy of this motion was served upon all counsel of record.

Signature